



July 2008

FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL (FISCAM)

Exposure Draft

This Exposure Draft of the FISCAM was superseded by GAO-09-232G, February 2, 2009. The FISCAM is available only in electronic form at <http://www.gao.gov/products/GAO-09-232G> on GAO's Web page. Should you need additional information, please contact us at FISCAM@gao.gov or call Robert Dacey at (202) 512-7439 or Greg Wilshusen at (202) 512-6244.



G A O

Accountability * Integrity * Reliability

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

July 2008

TO AUDIT OFFICIALS, AGENCY CIOS, AND OTHERS
INTERESTED IN FEDERAL INFORMATION SYSTEM CONTROLS
AUDITING AND REPORTING

This letter transmits the exposure draft of the Government Accountability Office (GAO) *Federal Information System Controls Audit Manual* (FISCAM) for your review and comment. The FISCAM presents a methodology for performing information system (IS) control¹ audits of federal and other governmental entities in accordance with professional standards, and was originally issued in January 1999. We have updated the FISCAM for significant changes affecting IS audits.

GAO would like to thank the President's Council on Integrity and Efficiency (PCIE) and the state auditor community for their significant input into the development of this revised FISCAM.

Summary of Major Revisions to FISCAM

The exposure draft revisions reflect changes in (1) technology used by government entities, (2) audit guidance and control criteria issued by the National Institute of Standards and Technology (NIST), and (3) generally accepted government

¹ Information system (IS) controls consist of those internal controls that are dependent on information systems processing and include general controls (entitywide, system, and business process application levels), business process application controls (input, processing, output, master file, interface, and data management system controls), and user controls¹ (controls performed by people interacting with information systems).

Exposure Draft

auditing standards (GAGAS), as presented in *Government Auditing Standards* (also known as the “Yellow Book”).² The Federal Information System Controls Audit Manual (FISCAM) provides a methodology for performing information system (IS) control audits in accordance with GAGAS. However, at the discretion of the auditor, this manual may be applied on other than GAGAS audits. As defined in GAGAS, IS controls consist of those internal controls that are dependent on information systems processing and include general controls and application controls. This manual focuses on evaluating the effectiveness of such general and application controls. This manual is intended for both (1) auditors to assist them in understanding the work done by IS controls specialists, and (2) IS controls specialists to plan and perform the IS controls audit.

In addition, the FISCAM is consistent with the GAO/PCIE *Financial Audit Manual* (FAM). Also, the FISCAM control activities are consistent with and have been mapped to the NIST Special Publication 800-53.

The FISCAM, which is consistent with NIST and other criteria, is organized to facilitate effective and efficient IS control audits. Specifically, the methodology in the FISCAM incorporates:

- Top-down, risk based approach that considers materiality and significance in determining effective and efficient audit procedures.
- Evaluation of entitywide controls and their effect on audit risk.
- Evaluation of general controls and their pervasive impact on business process application controls.
- Evaluation of security management at all levels (entitywide, system, and business process application levels).
- A control hierarchy (control categories, critical elements, and control activities) to assist in evaluating the significance of identified IS control weaknesses.
- Groupings of control categories consistent with the nature of the risk.

² GAO, *Government Auditing Standards*, [GAO-07-162G](#) (Washington, D.C.: July 2007).

Exposure Draft

- Experience gained in GAO's performance and review of IS control audits, including field testing the concepts in this revised FISCAM.

As discussed above, this manual is organized in a hierarchical structure to assist the auditor in performing the IS controls audit. Chapter 3 (general controls) and Chapter 4 (business process application level controls) contain several control categories, which are groupings of related controls pertaining to similar types of risk. For each control category, the manual identifies critical elements—tasks that are essential for establishing adequate controls within the category. For each critical element, there is a discussion of the associated control activities that are generally necessary to achieve the critical element, as well as related potential control techniques and suggested audit procedures. This hierarchical structure facilitates the auditor's audit planning and the auditor's analysis of identified control weaknesses.

Because control activities are generally necessary to achieve the critical elements, they are generally relevant to a GAGAS audit unless the related control category is not relevant, the audit scope is limited, or the auditor determines that, due to significant IS control weaknesses, it is not necessary to assess the effectiveness of all relevant IS controls. Within each relevant control activity, the auditor should identify control techniques implemented by the entity and determine whether the control techniques, as designed, are sufficient to achieve the control activity, considering IS audit risk and the audit objectives. The auditor may be able to determine whether control techniques are sufficient to achieve a particular control activity without evaluating and testing all of the control techniques. Also, depending on IS audit risk and the audit objectives, the nature and extent of control techniques necessary to achieve a particular control objective will vary.

If sufficient, the auditor should determine whether the control techniques are implemented (placed in operation) and are operating effectively. Also, the auditor should evaluate the nature and extent of testing performed by the entity. Such information can assist in identifying key controls and in assessing risk, but the auditor should not rely on testing performed by the entity in lieu of appropriate

Exposure Draft

auditor testing. If the control techniques implemented by the entity, as designed, are not sufficient to address the control activity, or the control techniques are not effectively implemented as designed, the auditor should determine the effect on IS controls and the audit objectives.

Throughout the updated FISCAM, revisions were made to reflect today's networked environment. The nature of IS risks continues to evolve. Protecting government computer systems has never been more important because of the complexity and interconnectivity of systems (including Internet and wireless), the ease of obtaining and using hacking tools, the steady advances in the sophistication and effectiveness of attack technology, and the emergence of new and more destructive attacks.

In addition, the FISCAM includes narrative that is designed to provide a basic understanding of the methodology (Chapter 2), general controls (Chapter 3) and business process application controls (Chapter 4) addressed by the FISCAM. The narrative may also be used as a reference source by the auditor and the IS control specialist. More experienced auditors and IS control specialists may find it unnecessary to routinely refer to such narrative in performing IS control audits. For example, a more experienced auditor may have sufficient knowledge, skills, and abilities to directly use the control tables in Chapters 2 and 3 (which are summarized in Appendices II and III).

Exposure Draft

A summary of significant changes to FISCAM is presented on the pages 6-10.

Instructions for Commenting on the Exposure Draft

The exposure draft of FISCAM is available only in electronic form at <http://www.gao.gov/cgi-bin/getrpt?rptno=GAO-08-1029G> on GAO's Web page. We request comments from federal audit officials, CIOs, financial managers, the public accounting profession, and other interested parties. Please associate your comments with specific references to section, paragraph, and page number. Also, please provide the rationale for your comments and proposed changes, along with suggested revised language. Please send your comments electronically to FISCAM@gao.gov no later than September 5, 2008. We anticipate that the final version of FISCAM will be issued in the fall of 2008 for use in conducting fiscal year 2009 federal financial statement audits.

Should you need additional information, please call Greg Wilshusen at (202) 512-6244; David Irvin at (214) 777-5643; or me at (202) 512-7439.

Sincerely yours,

A handwritten signature in black ink that reads "Robert F. Dacey". The signature is written in a cursive style with a large, sweeping flourish at the end of the name.

Robert F. Dacey
Chief Accountant
U.S. Government Accountability Office

Attachment and enclosures

Exposure Draft

SUMMARY OF SIGNIFICANT CHANGES TO THE FISCAM

Chapter 1

- Expanded purpose
 - provide guidance for performing effective and efficient Information System (IS) controls audits, either alone or as part of a performance audit, a financial audit, or an attestation engagement, including communication of any identified IS control weaknesses; and
 - inform financial, performance, and attestation auditors about IS controls and related audit issues, so that they can (1) plan their work in accordance with Generally Accepted Government Auditing Standards (GAGAS) and (2) integrate the work of IS controls specialists with other aspects of the financial or performance audit or attestation engagement.

- Conformity with July 2007 Revision to *Government Auditing Standards* – (“Yellow Book”)(GAGAS), including information system control categories

- Conformity with AICPA auditing standards, including new risk standards

- An overall framework of IS control objectives (see summary on pages 11-13)

Exposure Draft

Chapter 2

- IS audit methodology consistent with GAGAS and FAM, including planning, testing, and reporting phases (see a summary of methodology steps on pages 14-15), which incorporates:
 - A top-down, risk-based evaluation that considers materiality and significance in determining effective and efficient audit procedures (the auditor determines which IS control techniques are relevant to the audit objectives and which are necessary to achieve the control activities; generally, all control activities are relevant unless the audit scope is limited or the auditor determines that, due to significant IS control weaknesses, it is not necessary to test all relevant IS controls).
 - An evaluation of entitywide IS controls and their effect on audit risk, and therefore on the extent of audit testing (effective entitywide IS controls can reduce audit risk, while ineffective entitywide IS controls result in increased audit risk and generally are a contributory cause of IS control weaknesses at the system and business process application levels)—NIST SP 800-53 principally relates to controls at the system and application level.
 - An evaluation of general controls and their pervasive impact on business process application controls (effective general controls support the effectiveness of business process application controls, while ineffective general controls generally render business process application controls ineffective).
 - An evaluation of security management at all levels of control—entitywide, system (includes networks, operating systems, and infrastructure applications), and business process application levels.
 - A control hierarchy (control categories, critical elements, and control activities) to assist in evaluating the significance of identified IS control weaknesses (if a critical element is not achieved, the respective control category is not likely to be achieved; if one of the nine control categories are not

Exposure Draft

- effectively achieved, IS controls are ineffective, unless other factors sufficiently reduce the risk).
- Groupings of control categories consistent with the nature of the risk.
- Change from “installation level” general controls to “system level” general controls to reflect the logically networked structure of today’s systems
- IS controls audit documentation guidance for each audit phase
- Additional audit considerations that may affect an IS audit, including:
 - information security risk factors
 - automated audit tools
 - sampling techniques

Chapter 3

- Reorganized general control categories, consistent with GAGAS:
 - Security management - broadened to consider statutory requirements and best practices
 - Access controls - restructured to incorporate system software, eliminate redundancies, and facilitate IS auditing in a networked environment:
 - System boundaries
 - Identification and authentication
 - User authorization
 - Sensitive system resources
 - Audit and monitoring
 - Physical security
 - Configuration management - broadened to include network components and applications
 - Segregation of Duties - relatively unchanged
 - Contingency Planning - updated for new terminology

Exposure Draft

- Updated general control activities that (1) are consistent with current NIST and OMB information security guidance (particularly NIST Special Publication 800-53) including references/mapping of each critical element to such guidance, and (2) consider new IS risks and audit experience

Chapter 4

- Audit methodology and IS controls for business process applications that (1) are consistent with GAGAS and current NIST and OMB information security guidance (particularly NIST Special Publication 800-53) including references/mapping to such guidance, and (2) consider new IS risks and audit experience:
 - Application security (formerly general controls at the application level)
 - Business process controls related to the validity, completeness, accuracy, and confidentiality of transactions and data during application processing
 - Transaction data input
 - Transaction data processing
 - Transaction data output
 - Master file data setup and maintenance
 - Interface controls
 - Data management systems controls

Exposure Draft

Appendices

- Expanded appendices to support IS audits
 - Updated information system controls audit planning checklist
 - Tables for summarizing the results of the IS audit
 - Mapping of FISCAM to NIST Special Publication 800-53
 - Knowledge, skills, and abilities needed to perform IS audits
 - Scope of an IS audit in support of a financial audit
 - Entity's use of service organizations
 - Application of FISCAM to Single Audits
 - Application of FISCAM to FISMA
 - Complete FISMA text
 - Information System Controls Audit Documentation
 - Updated Glossary

Exposure Draft

INFORMATION SYSTEM CONTROLS OBJECTIVES

GENERAL CONTROLS

Security Management

Controls provide reasonable assurance that security management is effective, including effective:

- security management program
- periodic assessments and validation of risk,
- security control policies and procedures,
- security awareness training and other security-related personnel issues,
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices,
- remediation of information security weaknesses, and
- security over activities performed by external third parties.

Access Controls

Controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals, including effective

- protection of information system boundaries,
- identification and authentication mechanisms,
- authorization controls,
- protection of sensitive system resources,
- audit and monitoring capability, including incident handling, and
- physical security controls.

Exposure Draft

Configuration Management

Controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended, including effective

- configuration management policies, plans, and procedures,
- current configuration identification information,
- proper authorization, testing, approval, and tracking of all configuration changes,
- routine monitoring of the configuration,
- updating software on a timely basis to protect against known vulnerabilities, and
- documentation and approval of emergency changes to the configuration.

Segregation of Duties

Controls provide reasonable assurance that incompatible duties are effectively segregated, including effective

- segregation of incompatible duties and responsibilities and related policies, and
- control of personnel activities through formal operating procedures, supervision, and review.

Contingency Planning

Controls provide reasonable assurance that contingency planning (1) protects information resources and minimizes the risk of unplanned interruptions and (2) provides for recovery of critical operations should interruptions occur, including effective

- assessment of the criticality and sensitivity of computerized operations and identification of supporting resources,
- steps taken to prevent and minimize potential damage and interruption,
- comprehensive contingency plan, and
- periodic testing of the contingency plan, with appropriate adjustments to the plan based on the testing.

Exposure Draft

BUSINESS PROCESS APPLICATION CONTROLS

Completeness – controls provide reasonable assurance that all transactions that occurred are input into the system, accepted for processing, processed once and only once by the system, and properly included in output.

Accuracy – controls provide reasonable assurance that transactions are properly recorded, with correct amount/data, and on a timely basis (in the proper period); key data elements input for transactions are accurate; data elements are processed accurately by applications that produce reliable results; and output is accurate.

Validity – controls provide reasonable assurance (1) that all recorded transactions and actually occurred (are real), relate to the organization, are authentic, and were properly approved in accordance with management's authorization; and (2) that output contains only valid data.

Confidentiality – controls provide reasonable assurance that application data and reports and other output are protected against unauthorized access.

Exposure Draft

IS AUDIT METHODOLOGY STEPS

Plan the Information System Controls Audit

- Understand the Overall Audit Objectives and Related Scope of the Information System Controls Audit
- Understand the Entity's Operations and Key Business Processes.
- Obtain a General Understanding of the Structure of the Entity's Networks
- Identify Key Areas of Audit Interest
- Assess Information System Risk on a Preliminary Basis
- Identify Critical Control Points
- Obtain a Preliminary Understanding of Information System Controls
- Perform Other Audit Planning Procedures
 - Relevant Laws and Regulations
 - Consideration of the Risk of Fraud
 - Audit Resources
 - Multiyear Testing Plans
 - Communication with Entity Management and Those Charged with Governance
 - Service Organizations
 - Using the Work of Others
 - Audit Plan

Perform Information System Controls Audit Tests

- Understand Information Systems Relevant to the Audit Objectives
- Determine which IS Control Techniques are Relevant to the Audit Objectives
- For each Relevant IS Control Technique Determine Whether it is Suitably Designed to Achieve the Critical Activity and has been Implemented

Exposure Draft

- Perform Tests to Determine Whether such Control Techniques are Operating Effectively
- Identify Potential Weaknesses in IS Controls and Consider Compensating Controls

Report Audit Results

- Evaluate the Effects of Identified IS Control Weaknesses
 - Financial Audits, Attestation Engagements, and Performance Audits
- Consider Other Audit Reporting Requirements and Related Reporting Responsibilities

Exposure Draft

Contents

Chapter 1. Introduction.....	32
1.0 Chapter 1 Overview.....	32
1.1 Purpose and Anticipated Users of the Manual	34
1.2 Nature of Information System Controls	38
1.3 Determining the Nature and Extent of Audit Procedures.....	42
1.4 Organization of This Manual	43
1.4.1 Appendices	48
Chapter 2. Performing the Information System Controls Audit.....	50
2.0 Introduction	50
2.1 Planning the Information System Controls Audit	51
2.1.1 Overview.....	51
2.1.2 Understand the Overall Audit Objectives and Related Scope of the Information System Controls Audit.....	55
2.1.3 Understand the Entity’s Operations and Key Business Processes	57
2.1.4 Obtain a General Understanding of the Structure of the Entity’s Networks.....	62
2.1.5 Identify Key Areas of Audit Interest.....	62
2.1.6 Assess Information System Risk on a Preliminary Basis.....	63
2.1.7 Identify Critical Control Points.....	72
2.1.8 Obtain a Preliminary Understanding of Information System Controls.....	76
2.1.9 Perform Other Audit Planning Procedures	79
2.1.9.A Relevant Laws and Regulations	80
2.1.9.B Consideration of the Risk of Fraud	82

Exposure Draft

2.1.9.C Audit Resources	85
2.1.9.D Multiyear Testing Plans.....	87
2.1.9.E Communication with Entity Management and Those Charged with Governance.....	88
2.1.9.F Service Organizations	89
2.1.9.G Using the Work of Others	90
2.1.9.H Audit Plan	91
2.1.10 Documentation of Planning Phase	92
2.2 Perform Information System Controls Audit Tests.....	96
2.2.1 Overview	96
2.2.2 Appropriateness of Control Tests	109
2.2.3 Documentation of Control Testing Phase	111
2.3 Report Audit Results	112
2.3.1 Financial Audits and Attestation Engagements.....	116
2.3.2 Performance Audits	119
2.3.3 Other Audit Reporting Considerations	121
2.3.4 Related Reporting Responsibilities	123
2.3.5 Documentation of Reporting Phase	125
2.4 Documentation	126
2.5 Other Information System Controls Audit Considerations	128
2.5.1 Additional IS Risk Factors.....	129
2.5.1.A Defense-In-Depth Strategy.....	129
2.5.1.B Web Applications	131
2.5.1.C ERP Systems.....	131
2.5.1.D Interface Controls.....	133
2.5.1.E Database Management Systems.....	134
2.5.1.F Network-based Access Control Systems	134
2.5.1.G Workstations	135
2.5.2 Automated Audit Tools.....	135
2.5.3 Use of Sampling Techniques	138

Exposure Draft

Chapter 3. Evaluating and Testing

General Controls.....	139
3.0 Introduction	139
3.1. Security Management (SM).....	143
Security Program Guidance	144
Security Management Critical Elements	146
Critical Element SM-1: Establish a Security Management Program.....	146
SM-1.1. The security management program is adequately documented, approved, and up-to-date	147
SM-1.2. A security management structure has been established.....	149
SM-1.3. Information security responsibilities are clearly assigned.....	151
SM-1.4. Subordinate security plans are documented, approved, and kept up-to-date	153
SM-1.5. An inventory of systems is developed, documented, and kept up-to-date.....	154
Control Techniques and Suggested Audit Procedures for Critical Element SM-1	155
Critical Element SM-2. Periodically assess and validate risks	157
Control Techniques and Suggested Audit Procedures for Critical Element SM-2	164
Critical Element SM-3. Document security control policies and procedures.....	165
Control Techniques and Suggested Audit Procedures for Critical Element SM-3	167
Critical Element SM-4. Implement effective security awareness and other security-related personnel policies.....	167
SM-4.1 Ensure that resource owners, system administrators, and users are aware of security policies.....	169

Exposure Draft

SM-4.2. Hiring, transfer, termination, and performance policies address security	170
SM-4.3. Employees have adequate training and expertise	171
Control Techniques and Suggested Audit Procedures for Critical Element SM-4	172
Critical Element SM-5. Monitor the effectiveness of the security program	173
Control Techniques and Suggested Audit Procedures for Critical Element SM-5	183
Critical Element SM-6. Effectively Remediate Information Security Weaknesses.....	184
Control Techniques and Suggested Audit Procedures for Critical Element SM-6	185
Critical Element SM-7. Ensure that activities performed by external third parties are adequately secure	185
Control Techniques and Suggested Audit Procedures for Critical Element SM-7	188
3.2. Access Controls (AC).....	189
Critical Element AC-1. Adequately protect information system boundaries	194
AC-1.1. Appropriately control connectivity to system resources	196
AC-1.2. Appropriately control network sessions.....	201
Control Techniques and Suggested Audit Procedures for Critical Element AC-1	202
Critical Element AC-2. Implement effective identification and authentication mechanisms.....	205
AC-2.1. Users are appropriately identified and authenticated.....	206
Control Techniques and Suggested Audit Procedures for Critical Element AC-2	210
Critical Element AC-3. Implement effective authorization controls.....	212

Exposure Draft

AC-3.1. User accounts are appropriately controlled.....	212
AC-3.2. Processes and services are adequately controlled.....	216
Critical Element AC-4. Adequately protect sensitive system resources	220
AC-4.1. Access to sensitive system resources is restricted and monitored.....	221
AC-4.2. Adequate media controls have been implemented.....	226
AC-4.3. Cryptographic controls are effectively used	228
Control Techniques and Suggested Audit Procedures for Critical Element AC-4	231
Critical Element AC-5. Implement an effective audit and monitoring capability.....	234
AC-5.1. An effective incident response program is documented and approved.....	235
AC-5.2. Incidents are effectively identified and logged.....	238
AC-5.3. Incidents are properly analyzed and appropriate actions taken.....	240
Control Techniques and Suggested Audit Procedures for Critical Element AC-5	243
Critical Element AC-6. Establish adequate physical security controls	245
AC-6.1. Establish a physical security management program based on risk	246
AC-6.2. Establish adequate perimeter security based on risk	248
AC-6.3. Establish adequate security at entrances and exits based on risk	249
AC-6.4. Establish adequate interior security based on risk	249
AC-6.5. Adequately protect against emerging threats based on risk.....	250

Exposure Draft

Control Techniques and Suggested Audit Procedures for Critical Element AC-6	251
3.3. Configuration Management (CM).....	256
Critical Element CM-1. Develop and document CM policies, plans, and procedures	260
Control Techniques and Suggested Audit Procedures for Critical Element CM-1.....	263
Critical Element CM-2. Maintain current configuration identification information	263
Control Techniques and Suggested Audit Procedures for Critical Element CM-2.....	265
Critical Element CM-3. Properly authorize, test, approve, track, and control all configuration changes	265
Control Techniques and Suggested Audit Procedures for Critical Element CM-3.....	271
Critical Element CM-4. Routinely monitor the configuration.....	274
Control Techniques and Suggested Audit Procedures for Critical Element CM-4.....	276
Critical Element CM-5. Update software on a timely basis to protect against known vulnerabilities	276
Vulnerability scanning	277
Patch management	277
Virus protection	279
Emerging threats	279
Noncurrent software	282
Software usage.....	282
Control Techniques and Suggested Audit Procedures for Critical Element CM-5.....	283
Critical Element CM-6. Appropriately document and approve emergency changes to the configuration	284
Control Techniques and Suggested Audit Procedures for Critical Element CM-6.....	285
3.4. Segregation of Duties (SD).....	286

Exposure Draft

Critical Element SD-1. Segregate incompatible duties and establish related policies.....	288
SD-1.1. Incompatible duties have been identified and policies implemented to segregate these duties.....	288
SD-1.2. Job descriptions have been documented.....	292
SD-1.3. Employees understand their duties and responsibilities.....	292
Control Techniques and Suggested Audit Procedures for Critical Element SD-1.....	292
Critical Element SD-2. Control personnel activities through formal operating procedures, supervision, and review	294
SD-2.1. Formal procedures guide personnel in performing their duties	295
SD-2.2. Active supervision and review are provided for all personnel	295
Control Techniques and Suggested Audit Procedures for Critical Element SD-2.....	296
3.5. Contingency Planning (CP).....	297
Critical Element CP-1. Assess the criticality and sensitivity of computerized operations and identify supporting resources	298
CP-1.1. Critical data and operations are identified and prioritized.....	299
CP-1.2. Resources supporting critical operations are identified and analyzed.....	300
CP-1.3. Emergency processing priorities are established.....	301
Control Techniques and Suggested Audit Procedures for Critical Element CP-1.....	301
Critical Element CP-2. Take steps to prevent and minimize potential damage and interruption.....	302
CP-2.1. Data and program backup procedures have been implemented.....	303

Exposure Draft

CP-2.2. Adequate environmental controls have been implemented	305
CP-2.3. Staff have been trained to respond to emergencies.....	305
CP-2.4. Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.....	306
Control Techniques and Suggested Audit Procedures for Critical Element CP-2.....	308
Critical Element CP-3. Develop and document a comprehensive contingency plan.....	310
CP-3.1. An up-to-date contingency plan is documented.....	312
CP-3.2. Arrangements have been made for alternate data processing, storage, and telecommunications facilities	313
Control Techniques and Suggested Audit Procedures for Critical Element CP-3.....	315
Critical Element CP-4. Periodically test the contingency plan and adjust it as appropriate.....	316
CP-4.1. The plan is periodically tested.....	317
CP-4.2. Test results are analyzed and the contingency plan is adjusted accordingly	317
Control Techniques and Suggested Audit Procedures for Critical Element CP-4.....	317
Chapter 4. Evaluating and Testing Business Process Application Controls	319
4.0 Overview	319
4.0.1 The Auditor's Consideration of Business Process Control Objectives.....	325
4.0.2 Steps in Assessing Business Process Application Level Controls	326
4.0.3 Plan the Information System Controls Audit of Business Process Application Level Controls.....	327

Exposure Draft

4.0.3.A Understand the overall audit objectives and related scope of the business process application control assessment	327
4.0.3.B Understand the entity's operations and key business processes	329
4.0.3.C Obtain a general understanding of the structure of the entity's networks	330
4.0.3.D Identify key areas of audit interest (files, applications, systems, locations).....	330
4.0.3.E Assess information system risk on a preliminary basis	331
4.0.3.F Identify critical control points.....	331
4.0.3.G Obtain a preliminary understanding of application controls.....	332
4.0.3.H Perform other audit planning procedures	337
4.0.4 Perform Information System Controls Audit Tests of Business Process Application Level Controls	337
4.0.5 Report Audit Results	338
4.1. Application Level General Controls (AS)	340
Critical Element AS-1. Implement effective application security management.	341
Establish an application security plan	342
Periodically assess and validate application security risks	343
Document and implement application security policies and procedures.....	343
Implement effective security awareness and other security-related personnel policies	344
Monitor the effectiveness of the security program	344
Effectively remediate information security weaknesses.....	346
Implement effective security-related personnel policies	346
Adequately secure, document, and monitor external third party activities.....	346

Exposure Draft

Critical Element AS-2. Implement effective application access controls.....	351
Adequately protect application boundaries	352
Implement effective identification and authentication mechanisms	352
Implement effective authorization controls.....	353
Adequately protect sensitive application resources	355
Implement an effective audit and monitoring capability	356
Establish adequate physical security controls.....	357
Critical Element AS-3 – Implement effective application configuration management.....	362
Critical Element – AS-4: Segregate user access to conflicting transactions and activities and monitor segregation	369
Critical Element – AS-5: Implement effective application contingency planning	373
Assess the criticality and sensitivity of the application.....	374
Take steps to prevent and minimize potential damage and interruption.	374
Develop and document an application contingency plan.....	375
Periodically test the contingency plan and adjust it as appropriate.	376
4.2. Business Process Controls (BP).....	380
Master Data vs. Transaction Data	381
Business Process Control Objectives	382
NIST Guidance	384
Business Process Control Critical Elements.....	384
BP-1 Transaction Data Input is complete, accurate, valid, and confidential (Transaction Data Input Controls).....	384
Implement an effective transaction data strategy and design.....	386

Exposure Draft

Establish Input Preparation (approval and review) Policies and Procedures	387
Build Data Validation and Edits within the Application	388
Implement Effective Auditing and Monitoring Capability.....	388
BP-2 Transaction Data Processing is complete, accurate, valid, and confidential (Transaction Data Processing Controls).....	393
Formal Transaction Processing Procedures.....	394
Effective auditing and monitoring capability.....	395
BP-3 Transaction data output is complete, accurate, valid, and confidential (Transaction Data Output Controls).....	399
Implementing a reporting strategy	401
Establishing security and controls over report generation and distribution.	402
BP-4 Master Data Setup and Maintenance is Adequately Controlled	404
Implementing an effective design of master data elements.....	405
Establishing master data maintenance procedures, including approval, review, and adequate support for changes to master data	406
Implementing an effective auditing and monitoring capability	407
4.3. Interface Controls (IN)	412
Critical Element IN-1: Implement an effective interface strategy and design.	415
Critical Element IN-2: Implement effective interface processing procedures.....	416
4.4 Data Management System Controls (DA)	420
Key Concepts - Database Management Systems	421
Authentication/Authorization	421
SQL Commands	423

Exposure Draft

System, Role, Object Privileges	423
Stored Procedures	425
Key Concepts – Middleware.....	425
Middleware Controls.....	426
Key Concepts – Cryptography	426
Key Concepts – Data Warehouse, Data Reporting and Data Extraction Software.....	427
Segregation of Duties.....	428
Control Activities.....	429

Appendices

Appendix I - Information System Controls Audit Planning Checklist	431
Appendix II - Tables for Summarizing Work Performed in Evaluating and Testing General and Business Process Application Controls	448
Appendix III - Tables for Assessing the Effectiveness of General and Business Process Application Controls.....	450
Appendix IV - Mapping of FISCAM to SP 800-53	461
Appendix V - Knowledge, Skills, and Abilities Needed to Perform Information System Controls Audits	473
Appendix VI - Scope of an Information System Controls Audit in Support of a Financial Audit.....	480
Appendix VII - Entity’s Use of Service Organizations.....	510
Appendix VIII - Application of FISCAM to Single Audits	517
Appendix IX - Application of FISCAM to FISMA	525
Appendix X - Federal Information Security Management Act of 2002 (FISMA).....	534
Appendix XI - Information System Controls Audit Documentation	561
Appendix XII - Glossary.....	566
Appendix XIII – Bibliography	603

Exposure Draft

Figures

Figure 1. An Example of Typical Networked Systems	34
Figure 2: Example of Router Control Dependencies	74
Figure 3. Example of Network Schematic Describing System Weaknesses.....	114
Figure 4. Layered Approach to Network Security.....	196
Figure 5. Layered Security Mitigates the Risk of Individual Cybersecurity Threats.....	282
Figure 6: Steps in Assessing IT Systems Controls in a Financial Statement Audit.....	508
Figure 7: Steps for Each Significant Application in Assessing Information System Controls in a Financial Statement Audit	509

Tables

Table 1: Control Categories Applicable at Different Levels of Audit	101
Table 2. General Control Categories Applicable at Different Levels of Audit	142
Table 3. Critical Elements for Security Management	146
Table 4. Security Controls to Include in System Security Plans.....	154
Table 5. Control Techniques and Suggested Audit Procedures for Critical Element SM-1: Establish a security management program	156
Table 6. NIST Impact Definitions for Security Objectives	161
Table 7 Control Techniques and Suggested Audit Procedures for Critical Element SM-2: Periodically assess and validate risks.....	164
Table 8. Control Techniques and Suggested Audit Procedures for Critical Element SM-3: Document security control policies and procedures	167
Table 9. Control Techniques and Suggested Audit Procedures for Critical Element SM-4: Implement effective security awareness and other security- related personnel policies	172
Table 10. Types of Security Testing	178

Exposure Draft

Table 11. Control Techniques and Suggested Audit Procedures for Critical Element SM-5: Monitor the effectiveness of the security program.....	183
Table 12. Control Techniques and Suggested Audit Procedures for Critical Element SM-6: Effectively remediate information ssecurity weaknesses.....	185
Table 13. Examples of Agency-Identified Risks to Federal Systems and Data Resulting from Reliance on Contractors.....	187
Table 14. Control Techniques and Suggested Audit Procedures for Critical Element SM-7: Ensure that activities performed by external third parties are adequately secure	188
Table 15. Critical Elements for Access Control.....	194
Table 16. Control Techniques and Suggested Audit Procedures for Critical Element AC-1: Adequately protect information system boundaries	202
Table 17. Control Techniques and Suggested Audit Procedures for Critical Element AC-2: Implement effective identification and authentication mechanisms.....	210
Table 18. Control Techniques and Suggested Audit Procedures for Critical Element AC-3: Implement effective authorization controls.....	219
Table 19. Control Techniques and Suggested Audit Procedures for Critical Element AC-4: Adequately protect sensitive system resources	232
Table 20. Control Techniques and Suggested Audit Procedures for Critical Element AC-5: Implement an effective audit and monitoring capability.....	243
Table 21. Control Techniques and Suggested Audit Procedures for Critical Element AC-6: Establish adequate physical security controls.....	252
Table 22. Critical Elements for Configuration Management.....	260
Table 23. Control Techniques and Suggested Audit Procedures for Critical Element CM-1: Develop and document CM policies, plans, and procedures.....	263
Table 24. Control Techniques and Suggested Audit Procedures for Critical Element CM-2: Maintain current configuration identification information.....	265

Exposure Draft

Table 25. Control Techniques and Suggested Audit Procedures for Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes	271
Table 26. Control Techniques and Suggested Audit Procedures for Critical Element CM-4: Routinely monitor the configuration	276
Table 27. Control Techniques and Suggested Audit Procedures for Critical Element CM-5: Update software on a timely basis to protect against known vulnerabilities.....	283
Table 28. Control Techniques and Suggested Audit Procedures for Critical Element CM-6: Appropriately document and approve emergency changes to the configuration.....	285
Table 29. Critical Elements for Segregation of Duties.....	288
Table 30. Control Techniques and Suggested Audit Procedures for Critical Element SD-1: Segregate incompatible duties and establish related policies	292
Table 31. Control Techniques and Suggested Audit Procedures for Critical Element SD-2: Control personnel activities through formal operating procedures, supervision, and review	296
Table 32. Critical Elements for Contingency Planning.....	298
Table 33. Control Techniques and Suggested Audit Procedures for Critical Element CP-1: Assess the criticality and sensitivity of computerized operations and identify supporting resources.....	301
Table 34. Control Techniques and Suggested Audit Procedures for Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption	308
Table 35: Types of Contingency-Related Plans.....	311
Table 36. Control Techniques and Suggested Audit Procedures for Critical Element CP-3: Develop and document a comprehensive contingency plan	315
Table 37. Control Techniques and Suggested Audit Procedures for Critical Element CP-4: Periodically test the contingency plan and adjust it as appropriate	318
Table 38. General and Application Control Categories Applicable at Different Levels of Audit	324

Exposure Draft

Table 39. Control Techniques and Suggested Audit Procedures for Critical Element AS-1: Implement effective application security management	348
Table 40. Control Techniques and Suggested Audit Procedures for Critical Element AS-2: Implement effective application access controls.....	357
Table 41. Control Techniques and suggested audit procedures for AS-3 - Implement Effective Application Configuration Management.....	364
Table 42. Control Techniques and Suggested Audit Procedures For Critical Element AS-4 - Segregate user access to conflicting transactions and activities and monitor segregation	370
Table 43. Control Techniques And Suggested Audit Procedures For Critical Element AS-5 – Maintain an effective contingency planning program.....	378
Table 44. Control Techniques And Suggested Audit Procedures For Critical Element BP-1 - Transaction Data Input is complete, accurate, valid, and confidential.....	389
Table 45. Control Techniques And Suggested Audit Procedures For Critical Element BP-2 Transaction Data Processing is complete, accurate, valid, and confidential.....	397
Table 46. Control Techniques And Suggested Audit Procedures For Critical Element BP-3 Transaction data output is complete, accurate, valid, and confidential.....	403
Table 47. Control Techniques And Suggested Audit Procedures For Critical Element BP-4 Master Data Setup and Maintenance is Adequately Controlled	408
Table 48. Control Techniques and Suggested Audit Procedures for Critical Element IN-1: Implement an effective interface strategy and design.	416
Table 49. Control Techniques And Suggested Audit Procedures For Critical Element Critical Element Critical Element IN-2: Implement effective interface processing procedures.....	418
Table 50. Control Techniques and Suggested Audit Procedures for Critical Element DA-1 - Implement an effective data management system strategy and design	429

Exposure Draft

Chapter 1. Introduction

1.0 Chapter 1 Overview

This manual provides a methodology for performing information system (IS) control audits in accordance with “generally accepted government auditing standards” (GAGAS), as presented in *Government Auditing Standards* (also known as the “Yellow Book”).³ However, at the discretion of the auditor, this manual may be applied on other than GAGAS audits. As defined in GAGAS, IS controls consist of those internal controls that are dependent on information systems processing and include general controls and application controls. This manual focuses on such general and application controls.

As computer technology has advanced, federal agencies and other government entities have become dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, ineffective IS controls can result in significant risk to a broad array of government operations and assets. For example,

- resources, such as payments and collections, could be lost or stolen;
- computer resources could be used for unauthorized purposes, including the launching of attacks on others;
- sensitive information, such as taxpayer data, Social Security records, medical records, other personally identifiable information, and proprietary business information, could be inappropriately added, deleted, read, copied, disclosed, or

³ GAO, *Government Auditing Standards*, [GAO-07-162G](#) (Washington, D.C.: July 2007).

Exposure Draft

modified for purposes such as espionage, identity theft, or other types of crime;

- critical operations, such as those supporting national defense and emergency services, could be disrupted;
- data could be modified or destroyed for purposes of fraud or disruption; and
- agency/entity missions could be undermined by embarrassing incidents that result in diminished confidence in an agency's ability to conduct operations and fulfill its responsibilities.

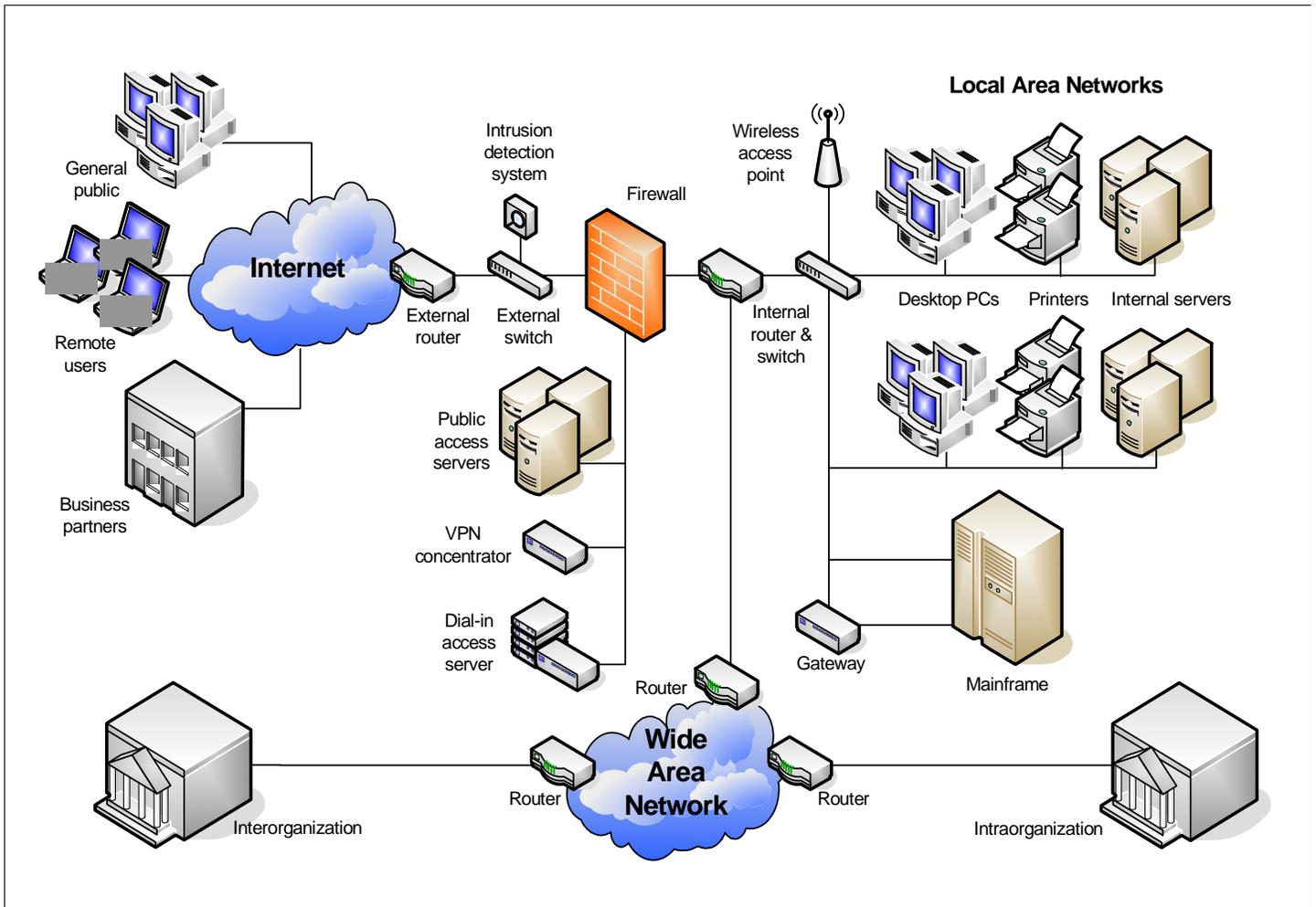
The nature of IS risks continues to evolve. Protecting government computer systems has never been more important because of the complexity and interconnectivity of systems (including Internet and wireless), the ease of obtaining and using hacking tools, the steady advances in the sophistication and effectiveness of attack technology, and the emergence of new and more destructive attacks.

As a result, the reliability of computerized data and of the systems that process, maintain, and report these data is a major concern to managements of government entities and their auditors. Auditors may need to evaluate the effectiveness of information system controls over data supporting financial statements or data used to analyze specific program costs and outcomes. In addition, auditors may be called on to evaluate the effectiveness of IS controls to help reduce the risk due to errors, fraud, and other illegal acts and disasters or other incidents that cause the systems to be unavailable.

Figure 1 illustrates the potential complexity of a typical networked infrastructure. Such infrastructures are built upon multiple hosts, including desktop personal computers (PCs), servers, and mainframes. Data communications links and network devices such as routers, hubs, and switches enable the hosts to communicate with one another through local area networks (LANs) within entities. Wide area networks (WANs) connect LANs at different geographical locations. Moreover, entities are typically connected to the Internet.

Exposure Draft

Figure 1. An Example of Typical Networked Systems



Sources: GAO analysis and Microsoft Visio™.

1.1 Purpose and Anticipated Users of the Manual

This manual describes (1) an audit methodology for assessing the effectiveness of IS controls, and (2) the IS controls that auditors evaluate when assessing the confidentiality, integrity, and availability of information and information systems. The Federal Information System Controls Audit Manual (FISCAM) is designed to be used primarily on financial and performance audits and

Exposure Draft

attestation engagements performed in accordance with “generally accepted government auditing standards” (GAGAS), as presented in *Government Auditing Standards* (also known as the “Yellow Book”). However, at the discretion of the auditor, this manual may be applied on other than GAGAS audits. This manual is intended for both (1) auditors performing financial and performance audits and attestation engagements to assist them in understanding the work done by IS controls specialists, and (2) IS controls specialists to plan and perform the IS controls audit. Federal and other government auditors may use this manual. It is not an auditing standard and it would be incorrect to refer to it as a standard. Its purposes are to

- provide guidance for performing effective and efficient IS controls audits, either alone or as part of a performance audit, a financial audit, or an attestation engagement, including communication of any identified IS control weaknesses; and
- inform financial, performance, and attestation auditors about IS controls and related audit issues, so that they can (1) plan their work in accordance with GAGAS and (2) integrate the work of IS controls specialists with other aspects of the financial or performance audit or attestation engagement.

The auditor should determine whether IS controls are relevant to the audit objectives. IS controls generally are relevant to a financial audit, as financial information is usually processed by information systems. For financial audits, the GAO/PCIE Financial Audit Manual (FAM)⁴ provides a framework for evaluating IS controls as part of a financial audit. The scope of an information system controls audit in support of a financial audit is summarized in Appendix VI. For performance audits, GAGAS 7.27 states that auditors should determine which audit procedures related to information system controls are needed to obtain sufficient, appropriate evidence to

⁴ The GAO/PCIE Financial Audit Manual (FAM) provides a framework for performing IS control audits performed as part of a financial audit. This framework is summarized in Appendix VI. The FAM is a joint effort between GAO and the President’s Council on Integrity and Efficiency (PCIE) to provide a methodology for performing financial audits that meets professional standards. It can be viewed or downloaded at <http://www.gao.gov/special.pubs/gaopcie/>.

Exposure Draft

support the audit findings and conclusions.⁵ This GAGAS paragraph provides factors that may assist auditors in making this determination.

This manual lists specific control activities and techniques and related suggested audit procedures. These are described at a high level and assume some level of expertise for an auditor to perform these audit procedures effectively. Accordingly, the auditor should develop more detailed audit steps based on the specific software and control techniques employed by the entity, the audit objectives, and significant areas of audit interest.

In addition, the FISCAM includes narrative that is designed to provide a basic understanding of the methodology (Chapter 2), general controls (Chapter 3) and business process application controls (Chapter 4) addressed by the FISCAM. The narrative may also be used as a reference source by the auditor and the IS control specialist. More experienced auditors and IS control specialists may find it unnecessary to routinely refer to such narrative in performing IS control audits. For example, a more experienced auditor may have sufficient knowledge, skills, and abilities to directly use the control tables in Chapters 2 and 3 (which are summarized in Appendices II and III).

Further, many of the suggested audit procedures start with the word “review.” The intent of such language is for the auditor to do more than simply look at the subject to be reviewed. Rather, a critical evaluation is envisioned, in which the auditor uses professional judgment and experience and undertakes the task with a certain level of skepticism, critical thinking, and creativity.

⁵ In addition, GAO guidance, “Assessing the Reliability of Computer-Processed Data” (Washington, DC; October 2002) can be used to assist the auditor in determining the use of IS control audits in assessing data reliability in a performance audit.

Exposure Draft

Although IS controls audit work, especially control testing, is generally performed by an IS controls specialist, financial or performance auditors with appropriate training, expertise, and supervision may undertake specific tasks in this area of the audit. Throughout this manual, the term “auditor” means either (1) an IS controls specialist or (2) a financial or performance auditor working in consultation with or under the supervision of an IS controls specialist. The FISCAM may be used by other staff that possess adequate IT competence. GAGAS requires that staff assigned to conduct an audit must collectively possess the technical knowledge, skills, and experience necessary to be competent for the type of work being performed. See Appendix V for additional information on the knowledge, skills, and abilities needed to perform information system control audits.

The following terms are used in the FISCAM to describe the degree of responsibility they impose on auditors and audit organizations:

- **must** - Auditors and audit organizations are required to comply with this unconditional requirement in all cases in which the circumstances exist to which the unconditional requirement applies. The term “must” is used only in FISCAM when the related requirement is specified as a “must” in GAGAS.
- **should** - Auditors and audit organizations are also required to comply with this presumptively mandatory requirement in all cases in which the circumstances exist to which the presumptively mandatory requirement applies; however, in rare circumstances, auditors and audit organizations may depart from a presumptively mandatory requirement provided they document their justification for the departure and how the alternative procedures performed in the circumstances were sufficient to achieve the objectives of the presumptively mandatory requirement. The term “should” is used when (1) the related requirement is specified as a “should” in GAGAS, or (2) performance is deemed necessary to meet GAGAS evidence requirements for an IS controls audit.
- **generally should** – Although optional, compliance with this policy is strongly encouraged.

Exposure Draft

- **may** – Compliance with this procedure or action is optional. It is descriptive rather than required. It is explanatory material that provides further explanation and guidance on the professional requirements or identifies and describes other procedures or actions relating to auditors’ or audit organizations’ activities.

When these or similar terms are used to describe management or entity actions (rather than actions of the auditor or audit organization), the general meaning of the terms is intended. If the entity does not comply with a “must” or “should”, the auditor should assess the impact of the noncompliance on the effectiveness of related IS controls.

1.2 Nature of Information System Controls

An evaluation of IS controls generally includes both general and business process application controls (also called application controls). The entity must have effective general and business process application controls to achieve the appropriate confidentiality, integrity, and availability of critical information and information systems.

Information system (IS) controls consist of those internal controls that are dependent on information systems processing and include general controls (entitywide, system, and business process application levels), business process application controls (input, processing, output, master file, interface, and data management system controls), and user controls⁶ (controls performed by people interacting with information systems). General and business process application controls are always IS controls. A user control is an IS control if its effectiveness depends on information systems processing or the reliability (accuracy, completeness, and validity) of information processed by information systems. Conversely, a user control is not an IS control if its effectiveness does not depend on information systems processing or the reliability of information processed by information systems.

⁶ User controls are portions of controls that are performed by people interacting with IS controls. The effectiveness of user controls typically depend on the accuracy of the information produced by the IS controls.

Exposure Draft

General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. Examples of primary objectives for general controls are to safeguard data, protect business process application programs, and ensure continued computer operations in case of unexpected interruptions. General controls are applied at the entitywide, system, and business process application levels. The effectiveness of general controls is a significant factor in determining the effectiveness of business process application controls, which are applied at the business process application level. Without effective general controls, business process application controls can generally be rendered ineffective by circumvention or modification. For example, automated edits designed to preclude users from entering unreasonably large dollar amounts in a payment processing system can be an effective application control. However, this control is not effective (cannot be relied on) if the general controls permit unauthorized program modifications that might allow some payments to be exempted from the edits or unauthorized changes to be made to data files after the edit is performed. GAGAS paragraph 7.23 discusses the following types of general controls: security management, logical and physical access, configuration management, segregation of duties, and contingency planning. Chapter 3 discusses the general controls in an IS controls audit and provides more detail on the critical elements of each type of general control.

Business process application controls are directly related to individual computerized applications. They help ensure that transactions are complete, accurate, valid, and confidential. Business process application controls include (1) programmed control techniques, such as automated edits, and (2) manual follow-up of computer-generated reports, such as reviews of reports identifying rejected or unusual items. GAGAS paragraph 7.23 defines application controls, or business controls, as those controls that help ensure the validity, completeness, accuracy, and confidentiality of transactions and data during application processing. Chapter 4 discusses the business process application level controls in an IS controls audit and provides more detail on the critical elements of each type of business process application control.

Exposure Draft

The overall framework of IS control objectives presented in the FISCAM can be viewed in different ways. One way to summarize the objectives is presented below.

GENERAL CONTROLS

Security Management

Controls provide reasonable assurance that security management is effective, including effective:

- security management program,
- periodic assessments and validation of risk,
- security control policies and procedures,
- security awareness training and other security-related personnel issues,
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices,
- remediation of information security weaknesses, and
- security over activities performed by external third parties.

Access Controls

Controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals, including effective:

- protection of information system boundaries,
- identification and authentication mechanisms,
- authorization controls,
- protection of sensitive system resources,
- audit and monitoring capability, including incident handling, and
- physical security controls.

Exposure Draft

Configuration Management

Controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended, including effective:

- configuration management policies, plans, and procedures,
- current configuration identification information,
- proper authorization, testing, approval, and tracking of all configuration changes,
- routine monitoring of the configuration,
- updating software on a timely basis to protect against known vulnerabilities, and
- documentation and approval of emergency changes to the configuration.

Segregation of Duties

Controls provide reasonable assurance that incompatible duties are effectively segregated, including effective:

- segregation of incompatible duties and responsibilities and related policies, and
- control of personnel activities through formal operating procedures, supervision, and review.

Contingency Planning

Controls provide reasonable assurance that contingency planning (1) protects information resources and minimizes the risk of unplanned interruptions and (2) provides for recovery of critical operations should interruptions occur, including effective:

- assessment of the criticality and sensitivity of computerized operations and identification of supporting resources,
- steps taken to prevent and minimize potential damage and interruption,
- comprehensive contingency plan, and
- periodic testing of the contingency plan, with appropriate adjustments to the plan based on the testing.

Exposure Draft

BUSINESS PROCESS APPLICATION CONTROLS

Completeness – controls provide reasonable assurance that all transactions that occurred are input into the system, accepted for processing, processed once and only once by the system, and properly included in output.

Accuracy – controls provide reasonable assurance that transactions are properly recorded, with correct amount/data, and on a timely basis (in the proper period); key data elements input for transactions are accurate; data elements are processed accurately by applications that produce reliable results; and output is accurate.

Validity – controls provide reasonable assurance (1) that all recorded transactions and actually occurred (are real), relate to the organization, are authentic, and were properly approved in accordance with management’s authorization; and (2) that output contains only valid data.

Confidentiality – controls provide reasonable assurance that application data and reports and other output are protected against unauthorized access.

1.3 Determining the Nature and Extent of Audit Procedures

The nature, timing, and extent of audit procedures performed to assess IS controls vary, depending on the audit objectives, the nature and extent of audit risks and other factors. Factors that can affect the nature, timing, and extent of audit procedures include the nature and complexity of the entity’s information systems, the entity’s control environment, and particular data and applications that are significant to the financial statements or operations of the entity. As appropriate, the IS controls specialist, and the financial, performance, or attestation auditor generally should work cooperatively to determine the nature, timing, and extent of IS controls audit procedures.

Inadequate coordination can result in ineffective auditing, for example, incomplete IS controls audits or improper consideration of

Exposure Draft

the work performed by the IS controls specialist. When performed as part of a financial statement audit, an assessment of IS controls is part of a comprehensive effort to evaluate both the controls over and reliability of financial reporting. In performance audits and attestation engagements, the nature and extent of IS controls audit procedures vary depending on the objectives of the audit.

1.4 Organization of This Manual

This manual is organized as follows:

- Chapter 2 describes the methodology for performing the IS controls audit.
- Chapter 3 provides information concerning the five general control categories, supporting critical elements, critical activities, potential control techniques, and suggested audit procedures.
- Chapter 4 provides information concerning the four business process application control level categories, supporting critical elements, critical activities, potential control techniques, and suggested audit procedures.
- Appendices provide supplemental information to assist the auditor in applying the FISCAM methodology.

This manual provides a risk-based approach for performing the information system controls audit that is consistent with government auditing standards and the GAO/PCIE *Financial Audit Manual* (FAM).⁷ The FISCAM is consistent with GAGAS and, where appropriate, the FISCAM discusses the applicable GAGAS requirements. Each of the nine control categories (five general control categories and four business process level control categories) represents a grouping of related controls having similar types of risk. For each category, this manual discusses the key underlying concepts, associated risks if the controls in the category

⁷The Financial Audit Manual is a joint effort between GAO and the President's Council on Integrity and Efficiency (PCIE) to provide a methodology for performing financial audits that meets professional standards. It can be viewed or downloaded at <http://www.gao.gov/special.pubs/gaopcie/>.

Exposure Draft

are ineffective, and the critical elements that should be achieved for IS controls to be effective.

This organization structure facilitates the following:

- **Audit planning:** Related audit steps can be grouped and broken down into three primary levels: the entitywide level, the system level, and the application level.
- **Evaluation of findings:** The effectiveness of IS controls can be evaluated by control technique, control activity, critical element, and control category.
- **Audit report drafting:** Findings can be summarized by control category and critical element.

To evaluate IS controls, the auditor should use appropriate criteria that are relevant to the audit objectives. For audits of federal entities, criteria are provided by the Federal Information Security Management Act (FISMA) (see Appendix X) and, for non-national security systems, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems* and other NIST guidance. The Office of Management and Budget (OMB) requires federal entities to apply other NIST guidance to non-national security systems. Also, other sources, such as vendor recommended IS practices and other generally accepted IS resources, may provide criteria.⁸ In addition, NIST is responsible for developing minimum security standards and guidelines that are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems.

⁸ The Security Content Automation Program (SCAP) is a joint program of the National Security Agency (NSA), Defense Information Systems Agency (DISA), and NIST. SCAP is designed as a free, public repository of tools to be used for automating technical control compliance activities, vulnerability checking, and security measurement. Such tools can provide additional criteria. See <http://nvd.nist.gov/scap/scap.cfm>.

Exposure Draft

FISMA states that standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President. Also, FISMA states that the head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency:

- provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;
- implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and
- complies with the requirements of FISMA.

GAO has consulted with NIST, as provided for in FISMA, and the FISCAM is mapped to NIST SP 800-53. Appendix IV provides a mapping of the two documents. In addition, each critical element includes references to related NIST SP 800-53 controls. NIST SP 800-53 includes a table of the mapping. Also, to assist auditors, individual FISCAM control activities reference related NIST SP 800-53 controls. This manual provides additional narrative to assist the auditor in evaluating IS controls. In addition, FISCAM incorporates other NIST guidance, including, for example, NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, which includes coverage of programmatic areas such as information security governance, capital planning and investment control, and system development life cycle.

The FISCAM, which is consistent with NIST and other criteria, is organized to facilitate effective and efficient IS controls audits. Specifically, the methodology in the FISCAM incorporates:

- A top-down, risk-based evaluation that considers materiality and significance in determining effective and efficient audit procedures (the auditor determines which IS control techniques are relevant to the audit objectives and which are necessary to achieve the control activities; generally, all control activities are

Exposure Draft

relevant unless the audit scope is limited or the auditor determines that, due to significant IS control weaknesses, it is not necessary to test all relevant IS controls).

- An evaluation of entitywide IS controls and their effect on audit risk, and therefore on the extent of audit testing (effective entitywide IS controls can reduce audit risk, while ineffective entitywide IS controls result in increased audit risk and generally are a contributory cause of IS control weaknesses at the system and business process application levels)—NIST SP 800-53 principally relates to controls at the system and application level.
- An evaluation of general controls and their pervasive impact on business process application controls (effective general controls support the effectiveness of business process application controls, while ineffective general controls generally render business process application controls ineffective).
- An evaluation of security management at all levels of control (entitywide, system, and business process application levels).
- A control hierarchy (control categories, critical elements, and control activities) to assist in evaluating the significance of identified IS control weaknesses (if a critical element is not achieved, the respective control category is not likely to be achieved; if one of the nine control categories are not effectively achieved, IS controls are ineffective, unless other factors sufficiently reduce the risk).
- Groupings of control categories consistent with the nature of the risk.
- Experience gained in GAO's performance and review of IS control audits, including field testing the concepts in this revised FISCAM.

As discussed above, this manual is organized in a hierarchical structure to assist the auditor in performing the IS controls audit. Chapter 3 (general controls) and Chapter 4 (business process application level controls) contain several control categories, which are groupings of related controls pertaining to similar types of risk. For each control category, the manual identifies critical elements—tasks that are essential for establishing adequate controls within the category. For each critical element, there is a discussion of the associated objectives, risks, and control activities, as well as related potential control techniques and suggested audit procedures. This

Exposure Draft

hierarchical structure facilitates the auditor's audit planning and analysis of identified control weaknesses.

Because control activities are generally necessary to achieve the critical elements, they are generally relevant to a GAGAS audit unless the related control category is not relevant, the audit scope is limited, or the auditor determines that, due to significant IS control weaknesses, it is not necessary to assess the effectiveness of all relevant IS controls. Within each relevant control activity, the auditor should identify control techniques implemented by the entity and determine whether the control techniques, as designed, are sufficient to achieve the control activity, considering IS audit risk and the audit objectives. The auditor may be able to determine whether control techniques are sufficient to achieve a particular control activity without evaluating and testing all of the control techniques. Also, depending on IS audit risk and the audit objectives, the nature and extent of control techniques necessary to achieve a particular control objective will vary.

If sufficient, the auditor should determine whether the control techniques are implemented (placed in operation) and are operating effectively. Also, the auditor should evaluate the nature and extent of testing performed by the entity. Such information can assist in identifying key controls and in assessing risk, but the auditor should not rely on testing performed by the entity in lieu of appropriate auditor testing. As discussed later in this section, if the control techniques implemented by the entity, as designed, are not sufficient to address the control activity, or the control techniques are not effectively implemented as designed, the auditor should determine the effect on IS controls and the audit objectives.

The entity's management is responsible for implementing an appropriate system of cost-effective IS controls, including an effective monitoring program to provide management with reasonable assurance that IS controls are properly designed and effectively operating. The auditor's responsibility is to perform tests of the IS controls and provide conclusions on the results of such tests to support the audit objectives.

Exposure Draft

1.4.1 Appendices

The appendices to the FISCAM, summarized below, provide additional information to assist the auditor in performing the IS controls audit.

List of Appendices

Appendix	Description	Purpose
Appendix I	Information System Controls Audit Planning Checklist	To assist the auditor in requesting relevant background information.
Appendix II	Tables for Summarizing Work Performed in Evaluating and Testing General and Business Process Application Controls	To assist the auditor in summarizing work performed.
Appendix III	Tables for Assessing the Effectiveness of General and Business Process Application Controls	To assist the auditor in assessing and reporting on IS controls.
Appendix IV	Mapping of FISCAM to SP 800-53	To show correlation between FISCAM critical elements and NIST SP 800-53.
Appendix V	Knowledge, Skills, and Abilities Needed to Perform Information System Controls Audits	Skill sets necessary to perform the IS controls audit.
Appendix VI	Scope of an Information System Controls Audit in Support of a Financial Audit	To show relation of FISCAM to relevant FAM sections.
Appendix VII	Entity's Use of Service Organizations	Audit issues related to an entity's use of a service organization and use of FISCAM as a basis for performing a SAS 70 audit.
Appendix VIII	Application of FISCAM to Single Audits	Use of FISCAM to assess IS controls over compliance requirements and financial reporting in connection with a single audit.
Appendix IX	Application of FISCAM to FISMA	Use of FISCAM for the independent evaluation of a federal agency's information security program required by FISMA.
Appendix X	Federal Information Security Management Act of 2002 (FISMA)	Key legislation containing criteria for federal IS controls audits.
Appendix XI	Information System Controls Audit Documentation	Summarizes IS controls audit documentation

Exposure Draft

Appendix	Description	Purpose
Appendix XII	Glossary	Key terms used in the FISCAM.
Appendix XIII	Bibliography	List of information sources.

Exposure Draft

Chapter 2. Performing the Information System Controls Audit

2.0 Introduction

The information system (IS) controls audit involves the following three phases:

- **Planning:** The auditor determines an effective and efficient way to obtain the evidential matter necessary to achieve the objectives of the IS controls audit and the audit report. For financial audits, the auditor develops an audit strategy and an audit plan. For performance audits, the auditor develops an audit plan.
- **Testing:** The auditor tests the effectiveness of IS controls that are relevant to the audit objectives.
- **Reporting:** The auditor concludes on the effect of any identified IS control weaknesses on the audit objectives and reports the results of the audit, including any material weaknesses and other significant deficiencies.

Appendix VI provides the scope of an IS controls audit in support of a financial statement audit.

For each of the three phases, the auditor prepares appropriate audit documentation.

Exposure Draft

2.1 Planning the Information System Controls Audit

2.1.1 Overview

In planning the IS controls audit, the auditor uses the equivalent concepts of materiality (in financial audits) and significance⁹ (in performance audits) to plan both effective and efficient audit procedures. Materiality and significance are concepts the auditor uses to determine the planned nature, timing, and extent of audit procedures. The underlying principle is that the auditor is not required to spend resources on items of little importance; that is, those that would not affect the judgment or conduct of a reasonable user of the audit report, in light of surrounding circumstances. On the basis of this principle, the auditor may determine that some areas of the IS controls audit (e.g., specific systems) are not material or significant, and therefore warrant little or no audit attention.

Materiality and significance include both quantitative and qualitative factors in relation to the subject matter of the audit. Even though a system may process transactions that are quantitatively immaterial or insignificant, the system may contain sensitive information or provide an access path to other systems that contain information that is sensitive or otherwise material or significant. For example, an application that provides public information via a website, if improperly configured, may expose internal network resources, including sensitive systems, to unauthorized access. Materiality is

⁹ GAGAS paragraph 7.04 states that “the concept of significance assists auditors throughout a performance audit, including when deciding the type and extent of audit work to perform, when evaluating results of audit work, and when developing the report and related findings and conclusions. Significance is defined as the relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors. Such factors include the magnitude of the matter in relation to the subject matter of the audit, the nature and effect of the matter, the relevance of the matter, the needs and interests of an objective third party with knowledge of the relevant information, and the impact of the matter to the audited program or activity. Professional judgment assists auditors when evaluating the significance of matters within the context of the audit objectives.”

Exposure Draft

more fully discussed in the FAM in section 230 (Determine Planning, Design, and Test Materiality), and both terms are discussed further in GAGAS.

Planning occurs throughout the audit as an iterative process. (For example, based on findings from the testing phase, the auditor may change the planned audit approach, including the design of specific tests.) However, planning activities are concentrated in the planning phase, during which the objectives are to obtain an understanding of the entity and its operations, including its internal control, identify significant issues, assess risk, and design the nature, extent, and timing of audit procedures. To accomplish this, the methodology presented in this chapter includes guidance to help the auditor do the following:

- Understand the overall audit objectives and related scope of the IS controls audit
- Obtain an understanding of an entity and its operations and key business processes
- Obtain a general understanding of the structure of the entity's networks
- Identify key areas of audit interest (files, applications, systems, locations)
- Assess IS risk on a preliminary basis
- Identify critical control points (for example, external access points to networks)
- Obtain a preliminary understanding of IS controls
- Perform other audit planning procedures

Although each of these areas is discussed separately in this chapter, they are not generally performed as discrete, sequential steps. For example, the IS controls specialist may gather information related to several steps concurrently, such as through interviews with key information technology (IT) staff or through data requests, or may perform steps in a different sequence. The auditor performs planning to determine an effective and efficient way to obtain the evidential matter necessary to support the objectives of the IS controls audit and the audit report. The nature and extent of audit

Exposure Draft

planning procedures varies for each audit depending on several factors, including the entity's size and complexity, the auditor's experience with the entity, and the auditor's knowledge of the entity's operations.

A key to a high-quality audit, the senior members of the audit team should be involved in planning. The auditor should coordinate with the entity being audited and, if the IS controls audit is part of another audit, with senior members of the overall audit team. In addition, auditors generally should determine the needs of other auditors who plan to use the work being performed and consult with them in a timely manner, especially when making decisions involving significant judgment.

If the IS controls audit is performed as part of a financial audit, GAGAS require the auditor to obtain an understanding of internal control over financial reporting sufficient to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures based on that assessment. This includes performing risk assessment procedures to evaluate the design of controls relevant to an audit of financial statements and to determine whether they have been implemented. In obtaining this understanding, the auditor considers how an entity's use of information technology (IT) and manual procedures affect controls relevant to the audit. The auditor's responsibilities for considering internal control in a financial audit are described in more detail in the FAM.

If the IS controls audit is performed as part of a performance audit, GAGAS¹⁰ (para. 7.24) states that when information systems controls are determined to be significant to the audit objectives, auditors should then evaluate the design and operating effectiveness of such controls. This evaluation would include other information systems controls that impact the effectiveness of the significant controls or the reliability of information used in performing the significant controls. Auditors should obtain a sufficient understanding of

¹⁰ There is a section of GAGAS entitled "Information Systems Controls" (paras. 7.23-7.27)

Exposure Draft

information systems controls necessary to assess audit risk and plan the audit within the context of the audit objectives.

Additionally, GAGAS (para. 7.27) states that auditors should determine which audit procedures related to information systems controls are needed to obtain sufficient, appropriate evidence to support the audit findings and conclusions. It also provides the following factors to assist the auditor in making this determination:

- a.** The extent to which internal controls that are significant to the audit depend on the reliability of information processed or generated by information systems.
- b.** The availability of evidence outside the information system to support the findings and conclusions: It may not be possible for auditors to obtain sufficient, appropriate evidence without assessing the effectiveness of relevant information systems controls. For example, if information supporting the findings and conclusions is generated by information systems or its reliability is dependent on information systems controls, there may not be sufficient supporting or corroborating information or documentary evidence that is available other than that produced by the information systems.
- c.** The relationship of information systems controls to data reliability: To obtain evidence about the reliability of computer-generated information, auditors may decide to assess the effectiveness of information systems controls as part of obtaining evidence about the reliability of the data. If the auditor concludes that information systems controls are effective, the auditor may reduce the extent of direct testing of data.
- d.** Assessing the effectiveness of information systems controls as an audit objective: When assessing the effectiveness of information systems controls is directly a part of an audit objective, auditors should test information systems controls necessary to address the audit objectives. For example, the audit may involve the effectiveness of information systems controls related to certain systems, facilities, or organizations.

Exposure Draft

2.1.2 Understand the Overall Audit Objectives and Related Scope of the Information System Controls Audit

The nature, timing, and extent of IS controls audit procedures vary depending upon the audit objectives. For example, the IS controls audit

- may be performed as part of a financial or performance audit, or may be performed as a separate engagement;
- may comprehensively address an entire entity, a component, or a network, or may narrowly target an application, specific technology (e.g., wireless, operating system, etc.), or location; and/or
- may include all control objectives or only a subset of control objectives (e.g., general controls, business process controls, or selected components of them, such as focusing on an entity's security management program).

If achieving the audit objectives does not require an overall conclusion on the effectiveness of the entity's IS controls or relates only to certain components of the entity or a subset of controls, the auditor's assessment would not necessarily identify all significant IS control weaknesses that may exist. For example, a limited review of controls over a type of operating system may not identify any significant weaknesses, although there may be very significant weaknesses in other areas that the auditor is unaware of because the scope of the audit is limited. Consequently, the auditor should evaluate the potential limitations of the auditor's work on the auditor's report and the needs and expectations of users. The auditor may determine that, because the limitations are so significant, the auditor will (1) communicate the limitations to the management of the audited entity, those charged with governance, and/or those requesting the audit, and (2) clearly report such limitations on the conclusions in the audit report. For example, in reporting on an audit of an operating system, the auditor may determine that it is appropriate to clearly report that the scope of the assessment was limited to the operating system and that, consequently, additional IS control weaknesses may exist that could impact the effectiveness of IS controls related to the operating system and to the entity as a whole.

Exposure Draft

Based on the overall engagement objectives, the auditor should develop and document the objectives of the IS controls audit. Typical IS controls audit objectives include the following:

- To support financial statement audits by, for example, assessing the effectiveness of IS controls related to financial reporting. (Note: The assessment of IS controls generally occurs during the internal control phase of a financial statement audit.) This assessment affects the nature, timing, and extent of financial audit procedures to be performed, as well as provide timely recommendations for improvements in IS controls. In addition, it may cover the entire audit year or relate only to controls at a point in time, such as at the end of the fiscal year. The scope of an IS controls audit in support of a financial audit is described further in the FAM and in Appendix VI.
- To supplement IT performance audits by assessing the effectiveness of security within the context of a broader systems review.
- To support other performance audits, such as assessing data reliability or how well an information system protects the confidentiality, integrity, and availability of data and the effect of this level of protection on program performance.
- To determine the effectiveness of IS controls, not in support of another audit, so that any risks are identified. Such audits may be designed to provide a conclusion on the effectiveness of IS controls and describe any material weaknesses and other significant deficiencies, or merely describe any IS control weaknesses without an overall conclusion as to the effectiveness of IS controls.
- To support evaluation of IS controls as required by FISMA.
- To support single audits.

The auditor should also determine and document (such as in an audit strategy and audit plan) the appropriate scope of the IS controls audit, including

- the organizational entities to be addressed (e.g., entitywide, selected component(s), etc.);

Exposure Draft

- the breadth of the audit (e.g., overall conclusion on IS control effectiveness, review of a specific application or technology area, such as wireless or UNIX, etc.);
- the types of IS controls to be tested:
- general and/or business process application level controls to be tested, or selected components; or
- all levels of the entity's information systems, or selected levels (e.g., entitywide, system level, or business process application level, or selected components of them—for definitions of each level, see the section below entitled “2.2 Perform Information System Controls Audit Tests,”).

If the IS controls audit is performed as part of another audit, the auditor should understand the overall audit objectives and how the IS controls audit will integrate with the audit. The auditor should reach a common understanding of objectives with the audit team responsible for the overall audit.

2.1.3 Understand the Entity's Operations and Key Business Processes

The auditor should obtain and document an understanding of the entity sufficient to plan and perform the audit in accordance with applicable auditing standards and requirements. In planning the audit, the auditor obtains information that will provide an overall understanding of the entity, such as its mission, size and location, organization, business, strategies, risks, and internal control structure. Understanding the entity's operations in the planning process enables the auditor to identify, respond to, and resolve problems early in the audit.

The auditor's understanding of the entity includes:

- entity management and organization,
- external and internal factors affecting the entity's operations, and
- key business processes (defined below).

To plan the audit, the auditor obtains a general understanding of the entity's and the IT function's organizational structure, including key

Exposure Draft

members of entity and IT management. The auditor's main objective is to understand how the entity is managed and how the organization is structured.

The auditor should identify significant external and internal factors that affect the entity's operations, particularly IT. External factors might include (1) IT budget, (2) external systems users, (3) current political climate, and (4) relevant legislation. Internal factors might include (1) size of the entity, (2) number of locations, (3) structure of the entity (centralized or decentralized), (4) complexity of operations, (5) IT management structure, (6) impact of information systems on business operations, (7) qualifications and competence of key IT personnel, and (8) turnover of key IT personnel. The auditor should document any significant factors that could affect the IS controls audit, including the auditor's risk assessment.

The auditor should also obtain a general understanding of the entity's business processes, particularly those processes most closely related to the audit objectives. Business processes are the primary functions that the entity performs in accomplishing its mission. Examples of typical business processes in government entities include

- mission-related processes, typically at the program or subprogram level, such as education, public health, law enforcement, or income security;
- financial management processes, such as collections, disbursements, or payroll; and
- other support processes, such as human resources, property management, or security.

Exposure Draft

Understanding the entity's operations and business processes includes understanding how business process applications are used to support key business processes, as it tends to vary from entity to entity. The auditor should obtain and review documentation, such as design documents, blueprints, business process procedures, user manuals, etc., and inquire of knowledgeable personnel to obtain a general understanding of each significant business process application that is relevant to the audit objectives. This includes a detailed understanding of

- business rules (e.g. removing all transactions that fail edits or only selected ones based on established criteria),
- transaction flows (detailed study of the entity's internal controls over a particular category of events that identifies all key procedures and controls relating to the processing of transactions), and
- application and software module interaction (transactions leave one system for processing by another, e.g. payroll time card interfaces with pay rate file to determine salary information).

Obtaining this understanding is essential to assessing information system risk, understanding application controls, and developing relevant audit procedures. For efficiency, the auditor may combine this step with the steps in FISCAM section 2.2.1 subsection entitled "Understand Information Systems Relevant to the Audit Objectives" to aid in the identification of relevant controls.

The auditor should identify and document the key business processes that are relevant to the audit objectives. For each key business process, the auditor should identify the significant general support systems and major applications that are used to support

Exposure Draft

each key business process.¹¹ Also, for each key business process, the auditor should identify the use of contractors and others to process information and/or operate systems for or on behalf of the entity. Throughout the remainder of this manual, references to entity systems and business processes include the use of contractors and others to process information and/or operate systems for or on behalf of the entity. If the IS controls audit is performed as part of a financial audit, as discussed in FAM 320 (Understand Information Systems) and other FAM sections, the auditor should obtain an understanding of the entity's information systems (including methods and records) for processing and reporting accounting (including supplemental information), compliance, and operations data (including performance measures reported in the Management's Discussion and Analysis).

The auditor should document an understanding of the entity's operations and key business processes, including the following items to the extent relevant to the audit objectives:

- the significance and nature of the programs and functions supported by information systems;
- a general understanding of the entity's and the IT function's organizational structure;
- key business processes relevant to the audit objectives, including business rules, transaction flows, and application and software module interaction;
- significant general support systems and major applications that support each key business process;
- background information checklist, if used;
- significant internal and external factors that could affect the IS controls audit objectives;

¹¹ OMB uses the terms "general support" and "application" systems to describe the two types of entity systems. As defined in OMB Circular A-130, a general support system is an interconnected set of information resources under the same direct management control that share common functionality. It normally includes hardware, software, information, data, applications, communications, and people. The term "application" means the use of information resources (information and information technology) to satisfy a specific set of user requirements.

Exposure Draft

- a detailed organization chart, particularly the IT and the IS components;
- significant changes in the IT environment or significant applications implemented within the recent past (e.g. 2 years) or planned within the near future (e.g., 2 years); and
- the entity's reliance on third parties to provide IT services (e.g., in-house, remote connectivity, remote processing).

Appendix I includes an Information System Controls Audit Planning Checklist that can be provided to the entity's management to facilitate gathering appropriate information for this audit step.

The auditor generally gathers planning information through different methods (observation, interviews, reading policy and procedure manuals, etc.) and from a variety of sources, including

- previous audits and management reviews,
- top-level entity and IT management,
- entity management responsible for relevant significant programs,
- Office of Inspector General (IG) and internal audit management (including any internal control officer),
- other members of the audit organization, concerning relevant completed, planned or in-progress assignments,
- personnel in the Office of General Counsel, and
- personnel in the Special Investigator Unit.

Also, the auditor generally gathers information from relevant reports and articles issued by or about the entity, including

- GAO reports;
- IG, internal audit, or other audit reports (including those for performance audits and other reviews);
- congressional hearings and reports;
- consultant reports; and
- material published about the entity in newspapers, magazines, Internet sites, and other publications.

Exposure Draft

2.1.4 Obtain a General Understanding of the Structure of the Entity's Networks

The auditor should obtain and document a general understanding of the structure of the entity's networks as a basis for planning the IS controls audit. The auditor's understanding includes a high-level view of the network architecture that the entity uses to implement key business processes. Such an understanding helps the auditor to assess risk, identify potential critical control points on a preliminary basis, understand technologies that may be subject to audit, and identify key locations. The auditor generally should request documentation of such information from the entity, including both high-level and detailed network schematics. The auditor should obtain the following information about the network architecture, generally documented in network schematics:

- Internet presence;
- firewalls, routers, and switches;
- intrusion detection or prevention systems;
- critical systems, such as Web and mail systems, file transfer systems, etc.;
- network management systems;
- connections to inter- and intra-agency sites;
- connections to other external organizations;
- remote access—virtual private network and dial-in; and
- wireless connections.

2.1.5 Identify Key Areas of Audit Interest

The auditor should identify key areas of audit interest, which are those that are critical to achieving the audit objectives (e.g., general support and business process application systems and files (or components thereof)). For a financial audit, this would include key financial applications and data and related feeder systems.¹² For a performance audit, this would include key systems that are likely to

¹²A feeder system is a system that provides information or data to support the main application. For example, in a payroll system the time and attendance system is the feeder system for the main application.

Exposure Draft

be significant to the audit objectives. For each key area of audit interest, the auditor should document relevant general support systems and major applications and files, including (1) the operational locations of each key system or file, (2) significant components of the associated hardware and software (e.g., firewalls, routers, hosts, operating systems), (3) other significant systems or system level resources that support the key areas of audit interest, and (4) prior audit problems reported. The auditor should also identify all access paths into and out of the key areas of audit interest. By identifying the key systems, files, or locations, the auditor can concentrate efforts on them, and do little or no work associated with other areas. The auditor generally should prioritize important systems, files, or locations in order of importance to the audit objectives. The auditor may characterize these items by the sensitivity or significance of the information processed, dollar value of the transactions processed, or presence or number of key edits or other controls performed by a business process application.

2.1.6 Assess Information System Risk on a Preliminary Basis

Overview

The auditor should assess, on a preliminary basis, the nature and extent of IS risk that relates to the key areas of audit interest. IS risk is the likelihood that a loss of confidentiality, integrity, or availability could occur that would materially/significantly affect the audit objectives (e.g., for a financial audit, a material misstatement). Assessing IS risk involves evaluation of both the likelihood that such a loss of confidentiality, integrity, or availability could occur and the materiality or significance of a loss of confidentiality, integrity, or availability to the audit objectives. The auditor should document factors that significantly increase or decrease the level of IS risk and their potential impact on the effectiveness of information system controls.

Assessing IS risk relating to the audit is different from management's risk assessment. In assessing IS risk, the auditor is not required or expected to reperform management's risk assessment. Rather, the auditor assesses IS risk on a preliminary

Exposure Draft

basis using data that would be collected in the planning of audit (this includes using the entity's risk assessments and performing other audit procedures as outlined below). The auditor's risk assessment should reflect the impact of the effectiveness of IS controls on the audit objectives.

The auditor's assessment of IS risk affects the nature, timing, and extent of IS controls audit procedures. As IS risk increases, the auditor should perform more extensive or more effective tests of IS controls. For example, a significant number of Internet access points that are not centrally controlled increases IS risk. In this case, the auditor would expand the auditor's testing, as there are more potential access paths to the key areas of audit interest. Risk assessments prepared by the entity may serve as a useful tool to assist in the identification of IS risk. However, the auditor should not rely on them without performing audit procedures to identify and assess risk.

To develop a framework for analyzing IS risk, the auditor should consider IS risk in the context of the following three security objectives for information and information systems:

- Integrity—guarding against improper information modification or destruction, which includes ensuring information nonrepudiation¹³ and authenticity¹⁴. A loss of integrity is the unauthorized modification or destruction of information.
- Confidentiality—preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

¹³Nonrepudiation is assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. Nonrepudiation may not be necessary to evaluate integrity to meet an audit objective.

¹⁴Authenticity is the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. Authenticity may not be necessary to evaluate integrity to meet an audit objective.

Exposure Draft

- **Availability**—ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

In some instances, one or more of the security objectives may have more significance to the audit objectives than the others.

The auditor should identify factors or conditions that significantly increase or decrease IS risk. These factors are general in nature; the auditor uses judgment in determining (1) the extent of procedures to identify the risks and (2) the impact of such risks on the entity's operations and the audit objectives. Because this risk assessment involves the exercise of significant audit judgment, the auditor should use experienced audit team personnel to perform the risk assessment. Factors considered would include those related to inherent risk¹⁵ as well as those related to the control environment, risk assessment, communication, and monitoring components of internal control¹⁶. The auditor identifies such factors based on information obtained in the planning phase, primarily from understanding the entity's operations and key business processes, including significant IT processing performed outside the entity.

For each risk identified, the auditor should document the nature and extent of the risk; the conditions that gave rise to that risk; and the specific information or operations affected (if not pervasive). The auditor should also document compensating controls or other considerations that may mitigate the effects of identified risks.

The auditor should assess and document, on a preliminary basis, the nature and extent of IS risks for the information and information systems related to the key areas of audit interest, considering

¹⁵ Inherent risk is the likelihood that a loss of confidentiality, integrity, or availability could occur that would materially/significantly affect the audit objectives (e.g., for a financial audit, a material misstatement), assuming that there are no related internal controls.

¹⁶ Standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1) describes the five standards of internal control as: control environment, risk assessment, control activities, information and communications, and monitoring. The specific IS controls assessed in an IS controls audit are part of the control activities component.

Exposure Draft

confidentiality, integrity, and availability. The auditor should document the basis for the assessed risk and its potential impact on the audit objectives. For example, in a financial audit, the auditor should evaluate the possibility of a material misstatement as a result of a loss of confidentiality, integrity, or availability. As discussed above, risk assessments prepared by the entity may serve as a useful tool to assist the auditor in the identification of IS risks.

As noted above, IS risk includes the risk of loss of confidentiality, integrity, or availability. Such risk includes the potential impact of a loss to entity operations, assets, and individuals. However, depending on the audit objectives, the impact on the audit objectives could be greater or lesser. Federal agencies are required to use the following three levels to categorize their systems based on the potential impact of a breach of security on organizational operations, organizational assets, or individuals:¹⁷

- *Low.* The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.¹⁸ A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
- *Moderate.* The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a significant degradation in mission capability to an extent and

¹⁷ These risk levels are discussed further in National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication (FIPS PUB) 199 (December 2003).

¹⁸ Adverse effects on individuals may include, for example, loss of the privacy to which individuals are entitled under law.

Exposure Draft

duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

- *High.* The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

The auditor's assessment of IS risk may change as audit evidence is obtained. To determine whether audit procedures continue to be appropriate, the auditor should periodically reassess the IS risk during the audit. For example, the auditor may reassess the IS risk level at the end of the planning and testing phases, as well as when evidence is obtained that significantly affects the auditor's risk assessment. If IS risk changes during the audit, the auditor should make any necessary changes to the nature, timing, and extent of planned audit procedures.

Inherent Risk Factors

Information systems can introduce additional risk factors not present in a manual system. To properly assess IS risk, the auditor should (1) evaluate each of the following factors and (2) assess the overall impact of information systems on IS risk. The impact of these factors typically will be pervasive in nature.

- The nature of the hardware and software may affect IS risk, as illustrated below.
- The type of processing (online, batch oriented, or distributed) presents different levels of IS risk. Distributed networks enable

Exposure Draft

multiple computer processing units to communicate with each other, increasing the number of potential access points and the risk of unauthorized access to computer resources and possible data alteration. On the other hand, distributed networks may decrease the risk of data inconsistencies at multiple processing units if the units share a common database.

- Peripheral access devices or system interfaces can increase IS risk. For example, Internet or wireless access to a system increases the system's accessibility to additional persons and therefore increases the risk of unauthorized access to computer resources.
- Highly customized application software may have higher IS risk than vendor-supplied software that has been thoroughly tested and is in general commercial use. On the other hand, vendor-supplied software new to commercial use may not have been thoroughly tested or undergone client processing to a degree that would encounter existing flaws.
- Certain hardware and software may have more significant identified weaknesses than others.
- In certain systems (e.g., enterprise resource planning—ERP—systems¹⁹), the audit trails and supporting information produced by the systems may be limited in their usefulness (1) as a basis for applying certain types of controls or (2) as audit evidence.
- Highly decentralized applications, particularly Web applications, increase IS risk by adding complexity to IS and increasing potential vulnerabilities.
- The application of new technologies generally increases the risk that secure configurations of such technologies may not be well developed or tested, or that IT personnel may not properly implement security over such new technologies.
- The manner in which the entity's networks are configured can affect the related IS risk. For example, factors increasing IS risks include a significant number of Internet access points that are

¹⁹ERP systems consist of functional modules that support business requirements such as human resources, financials, or inventory control. The modules can be used individually or in conjunction with other modules as needed. The individual modules contain the business process necessary to complete their intended function.

Exposure Draft

not centrally controlled, networks that are not segmented to protect sensitive systems or information, use of technologies that are no longer supported, or lack of technologies that enhance security.

- The consistency of the entity's enterprise architecture and IT strategy with its business strategies can affect the proper planning and implementation of IT systems and related security.

Also, the following risk factors, discussed in FAM 260 (Identify Risk Factors) are relevant to both financial and performance audits:

- Uniform processing of transactions: Because information systems process groups of identical transactions consistently, any misstatements arising from erroneous computer programming will occur consistently in the same types of transactions. However, the risk of random processing errors is reduced substantially in information systems-based accounting systems.
- Automatic processing: The information system may automatically initiate transactions or perform processing functions. Evidence of these processing steps (and any related controls) may or may not be visible.
- Increased potential for undetected misstatements: Information systems use and store information in electronic form and require less human involvement in processing than manual systems. Without adequate controls, there is increased risk that individuals could gain unauthorized access to sensitive information and alter data without leaving visible evidence. Because information is in electronic form, changes to computer programs and data are not readily detectable. Also, users may be less likely to challenge the reliability of information systems output than manual reports.
- Existence, completeness, and volume of the audit trail: The audit trail is the evidence that demonstrates how a specific transaction was initiated, processed, and summarized. For example, the audit trail for a purchase could include a purchase order; a receiving report; an invoice; an entry in an invoice register (purchases summarized by day, month, and/or account); and general ledger postings from the invoice register. Some computer systems are designed to maintain the audit trail for only a short period, only

Exposure Draft

in an electronic format, or only in summary form. Also, the information generated may be too voluminous to be analyzed effectively without software. For example, one transaction may result from the automatic summarization of information from hundreds of locations. Without the use of audit or retrieval software, tracing transactions through the processing may be extremely difficult.

- Unusual or nonroutine transactions: As with manual systems, unusual or nonroutine transactions increase IS risk. Programs developed to process such transactions may not be subject to the same procedures as programs developed to process routine transactions. For example, the entity may use a utility program to extract specified information in support of a nonroutine management decision.

In addition, the auditor should evaluate the additional audit risk factors discussed in the “Additional IS Risk Factors” at the end of this chapter.

Risk Factors Related to the Control Environment, Risk Assessment, Communication, and Monitoring Components of Internal Control

Also, the auditor should evaluate the following IT system factors, to the extent relevant to the audit objectives, in making an overall assessment of the control environment, risk assessment, communication, and monitoring components of internal control.

a. Management's attitudes and awareness with respect to IT systems: Management's interest in and awareness of IT system functions (including those performed for the entity by other organizations) is important in establishing an organizationwide consciousness of control issues. Management may demonstrate its interest and awareness by

- considering the risks and benefits of computer applications;
- communicating policies regarding IT system functions and responsibilities;
- overseeing policies and procedures for developing, modifying, maintaining, and using computers, and for controlling access to programs and files;

Exposure Draft

- considering the risk of material misstatement, including fraud risk, related to IT systems;
- responding to previous recommendations or concerns;
- quickly and effectively planning for, and responding to, computerized processing crises; and
- using reliable computer-generated information for key operating decisions.

b. Organization and structure of the IT system function: The organizational structure affects the control environment. Centralized structures often have a single computer processing organization and use a single set of system and applications software, enabling tighter management control over IT systems. In decentralized structures, each computer center generally has its own computer processing organization, application programs, and system software, which may result in differences in policies and procedures and various levels of compliance at each location.

c. Clearly defined assignment of responsibilities and authority: Appropriate assignment of responsibility according to typical IT system functional areas can affect the control environment. Factors to consider include

- how the position of the Chief Information Officer (CIO) fits into the organizational structure;
- whether duties are appropriately segregated within the IT systems function, such as operators and programmers, since lack of segregation typically affects all systems;
- the extent to which management external to the IT systems function is involved in major systems development decisions; and
- the extent to which IT system policies, standards, and procedures are documented, understood, followed, and enforced.

d. Management's ability to identify and to respond to potential risk: Computer processing, by its nature, introduces additional risk factors. The entity should be aware of these risks and should develop appropriate policies and procedures to respond to any IT system issues that might occur. The auditor may evaluate

Exposure Draft

- the methods for monitoring incompatible functions and for enforcing segregation of duties and
- management’s mechanism for identifying and responding to unusual or exceptional conditions.

Examples of potential IT-related control environment, risk assessment, communication, and monitoring weaknesses include:

- Management and personnel in key areas (such as accounting, IT systems, IG, and internal auditing) have a high turnover.
- Management attitude toward IT systems and accounting functions is that these are necessary “bean counting” functions rather than a vehicle for exercising control over the entity's activities or making better decisions.
- The number of people, particularly in IT systems and accounting, with requisite skill levels relative to the size and complexity of the operations is inadequate.
- Management has not adequately identified risks arising from internal sources, such as human resources (ability to retain key people) or IT (adequacy of backup systems in the event of systems failure).
- Accounting systems and/or information systems, including IT systems, are not modified in response to changing conditions.

2.1.7 Identify Critical Control Points

The auditor should identify and document critical control points in the design of the entity’s information systems based on the auditor’s understanding of such systems, key areas of audit interest, and IS risk. Critical control points are those system control points that, if compromised, could allow an individual to gain unauthorized access to or perform unauthorized or inappropriate activities on entity systems or data, which could lead directly or indirectly to unauthorized access or modifications to the key areas of audit interest. Control points typically include external access points to the entity’s networks, interconnections with other external and internal systems, system components controlling the flow of information through the entity’s networks or to the key areas of audit interest, critical storage and processing devices, and related operating systems, infrastructure applications, and relevant

Exposure Draft

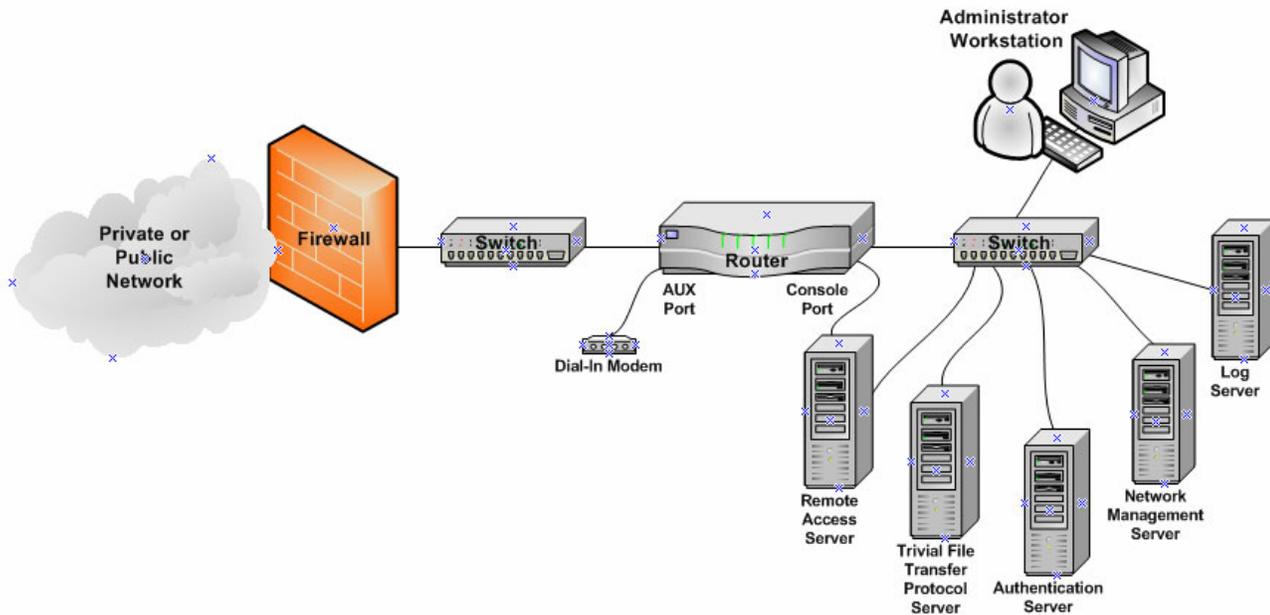
business process applications. Typical control points also include network components where business process application controls are applied. As the audit testing proceeds and the auditor gains a better understanding of the entity's information systems, of control weaknesses, and of the related risks, the auditor should periodically reassess the critical control points. Based on information obtained during audit planning, the auditor should identify those critical control points in the entity's IT systems that are significant to the effectiveness of security over the key areas of audit interest.

An analysis of critical control points includes consideration of alternate work sites. Since multiple FISCAM control categories are relevant to alternate work sites, it is not addressed as a specific control in this document. For further information on this subject refer to NIST guidance contained in SP 800-53 and SP 800-46.

In identifying critical control points and in planning and performing the assessment of IS controls, auditors apply the concept of control dependencies. A control dependency exists when the effectiveness of an internal control is dependent on the effectiveness of other internal controls. An assessment of the effectiveness of information system controls over a critical control point includes testing the effectiveness of controls over other control points upon which the security of the critical control point is dependent. Figure 2 illustrates the concept of a control dependency in relation to a router for a typical network.

Exposure Draft

Figure 2: Example of Router Control Dependencies



Source: GAO.

The figure illustrates that the effectiveness of controls over the router in this example network are dependent on controls over other control points. In this example, because unauthorized or inappropriate access to the other control points could affect the security of the router, the auditor's tests of IS controls generally should include controls over

- the trivial file transfer protocol (tftp) servers used to maintain a central repository of sensitive configuration files (tftp servers do not require authentication and are also used as remote boot devices for routers);
- the centralized authentication server that authenticates users to the router and other network devices;
- network switches that could share sensitive data with routers such as passwords and shared keys (also, network switches provide a trusted path to the routers);
- administrative workstations used to manage network devices, such as routers; and

Exposure Draft

- the log server, which maintains logs containing relevant information about significant network events, such as router access.

In addition, as part of a review of the system level controls over the router, the auditor generally should test controls over

- the network management servers used to manage configuration files that contain sensitive information about network devices such as routers;
- remote access to the router via the auxiliary and console ports that could be used to remotely manage the router;
- the firewalls that provide boundary protection (i.e., limits connectivity to the router);
- unencrypted network traffic that could be “sniffed” to obtain router or other privileged passwords; and
- the PC connected to the router that could facilitate direct connectivity to the router.

Further, the auditor generally should test other controls that may affect the security of the router, based on the auditor’s judgment. Note that, in addition to controls over access to the router itself, IS controls include controls over the routing of traffic throughout the network (see AC-1 in Chapter 3).

As the auditor performs the IS controls audit, based on the auditor’s assessment of risk and the results of audit tests, the auditor may determine that it is necessary to modify the scope of the audit. For example, if significant IS control weaknesses are identified during the audit, it may not be necessary to perform all planned tests of IS controls. If testing is reduced due to the identification of significant weaknesses, the auditor should document such a decision. Also, testing may result in the identification of additional risks, and critical control points, and /or control dependencies; the auditor should determine whether to adjust the scope for them.

Exposure Draft

2.1.8 Obtain a Preliminary Understanding of Information System Controls

The auditor should obtain and document a preliminary understanding of the design of the entity's IS controls, including the organization, staffing, responsibilities, authorities, and resources of the entity's security management function. The auditor should document a preliminary understanding of entitywide controls (or componentwide controls if only a component is being audited) related to security management, access controls, configuration management, segregation of duties and, contingency planning.

The auditor should understand the design of each of the three types of IS controls (general, business process application, and user controls) to the extent necessary to tentatively conclude whether these controls are likely to be effective. If they are likely to be effective, the auditor should consider specific IS controls in determining whether relevant IS control objectives are achieved. If IS controls are not likely to be effective, the auditor should obtain a sufficient understanding of control risks arising from IS controls to assess audit risk, design appropriate audit procedures, and develop appropriate findings.

In addition, the auditor should obtain a preliminary understanding of the business process application controls (business process, interface, and data management system controls) over key business process applications identified as or related to key areas of audit interest, determine where those controls are applied, and determine whether the controls are designed effectively and have been implemented (placed in operation). For example, authentication and authorization may be applied in network components that are different from those where key data files or applications reside; (e.g., Web applications that reside on one server may be used to authenticate and authorize users of legacy systems that run on different servers or systems). The auditor should determine the potential impact of any identified design weaknesses on the completeness, accuracy, validity, and confidentiality of related application data. (See Chapter 4 for a description of completeness, accuracy, validity, and confidentiality.)

The auditor should make a preliminary assessment of whether IS controls are likely to be effective to assist in determining the nature,

Exposure Draft

timing, and extent of testing. This assessment is based primarily on discussions with personnel throughout the entity, including program managers, system administrators, information resource managers, and systems security managers; on observations of IT operations and controls; on reviewing examples of evidence of control performance; on prior audits or the work of others; and on reading written policies and procedures. This preliminary assessment for financial audits is discussed further at FAM 270 (Determine Likelihood of Effective Information System Controls). Based on the preliminary assessment, the auditor should make any adjustments, as necessary, to the IS risk level, critical control points, and planned scope of the audit work.

Control activities for critical elements in each general control and business process control category are described in Chapters 3 and 4, respectively, and summarized in Appendix II. The auditor may use the summary tables in Appendix II, which are also available in electronic form from GAO (www.gao.gov), to document preliminary findings and to assist in making the preliminary assessment of controls. As the audit progresses through testing of internal controls, the auditor may continue to use the electronic version of the tables to document controls evaluated and tested, test procedures performed, conclusions, and supporting documentation references.

The auditor should include the following information in the documentation of their preliminary understanding of the design of IS controls, to the extent relevant to the audit objectives:

- An identification of relevant entitywide, system, and business process application level controls designed to achieve the control activities for each critical element within each general control area and a determination of whether they are designed effectively and implemented (placed in operation), including identification of control activities for which there are no or ineffective controls at the entitywide level and the related risks
- Identification of business process controls for key applications identified as key areas of audit interest, determination of where those controls are implemented within the entity's systems, and the auditor's conclusion about whether the controls are designed

Exposure Draft

effectively and implemented (placed in operation), including identification of control activities for which there are no or ineffective controls and the related risks and the potential impact of any identified design weaknesses on the completeness, accuracy, validity, and confidentiality of application data

- Any internal or third-party information systems reviews, audits, or specialized systems testing (e.g., penetration tests, disaster recovery tests, and application-specific tests) performed during the last year and the auditor's evaluation of the other auditor's objectivity, competence and conclusions
- Management's plans of action and milestones, or their equivalent, that identify corrective actions planned to address known IS control weaknesses
- Status of the prior years' audit findings
- Documentation for any significant computer security related incidents identified and reported for the last year
- Documented security plans
- Documented risk assessments for relevant systems (e.g., general support systems and major applications)
- System certification and accreditation documentation or equivalent for relevant systems
- Documented business continuity of operations plans and disaster recovery plans
- A description of the entity's use of third-party IT services

The auditor should obtain information from relevant reports and other documents concerning IS that are issued by or about the entity, including

- the entity's prior FISMA or equivalent reports on IS;
- the entity's annual performance and accountability report or equivalent reports on performance including reports filed to comply with the Federal Financial Management Improvement

Exposure Draft

Act of 1996²⁰ (FFMIA) and Federal Managers Financial Integrity Act of 1982²¹ (FMFIA);

- other reports by management or the auditor about IS;
- other reports that contain information concerning IS that are relevant to the audit objectives;
- GAO reports;
- IG and internal audit reports (including those for performance audits and other reviews); and
- consultant reports.

2.1.9 Perform Other Audit Planning Procedures

The auditor should address the following areas during the planning phase, even though related audit procedures may be applied during the other phases. More specifically, the auditor should address any other issues, not identified in the previous steps, that could affect the objectives, scope, or methodology of the IS controls audit, including

- relevant laws and regulations;
- the risk of fraud;
- staffing and other resources needed to perform the audit;
- multiyear testing plans;
- communication to management officials and those charged with governance concerning the planning and performance of the audit, and to others as applicable;
- use of service organizations;
- using the work of others; and
- preparation of an audit plan (and an audit strategy for financial statement audits).

²⁰ Federal Financial Management Improvement Act of 1996, 31 U.S.C. 3512 note.

²¹ Federal Managers' Financial Integrity Act of 1982 (FMFIA) 31 U.S.C. 3512 (c), (d).

Exposure Draft

2.1.9.A Relevant Laws and Regulations

The auditor should identify applicable laws and regulations that are relevant to IS at the entity. Such laws and regulations may establish general or specific IS control requirements or criteria. Laws and regulations generally relevant to audits of federal agencies include FISMA, FMFIA, FFMIA, Appendix III of OMB Circular A-130²², OMB Circular A-123²³, and FISMA implementing guidance. Specific federal laws and regulations that may affect the entity include:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA),²⁴
- Gramm-Leach-Bliley,²⁵
- Requirements for information security for Medicare Administrative Contractors,²⁶
- Chief Privacy Officer statutory requirements,²⁷
- OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*, and²⁸
- OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information*.²⁹

²² OMB, *Management of Federal Information Resources* (Washington, D.C.: November 28, 2000).

²³ OMB, *Management's Responsibility for Internal Control* (Washington, D.C.: December 21, 2004).

²⁴ Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 42 U.S.C. 1320d, et seq. (— 68 FR 8334 (2/20/03), HIPAA Security Standards and — 67 FR 53182 (Aug. 14, 2002), HIPAA Privacy Standards.

²⁵ Gramm-Leach-Bliley, Pub. L. 106-102 (Nov. 12, 1999), see, e.g., Title V, Privacy.

²⁶ Requirements for information security for Medicare Administrative Contractors, Sec. 912, Medicare Prescription Drug, Improvement, and Modernization Act of 2003, Pub. L. 108-173 (Dec. 8, 2003), 117 Stat. 2387.

²⁷ Chief Privacy Officer, sec. 522, Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005, Div. H, Omnibus Appropriations Act, 2005, Pub. L. 108-447 (Dec. 8, 2004), Cong. Rec. (Nov. 19, 2004), p. H10359.

²⁸ OMB, *Designation of Senior Agency Officials for Privacy*, (Washington, D.C.: Feb. 11, 2005).

Exposure Draft

- OMB Memorandum M 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.³⁰

In IS controls audits of state and local governments, the auditor should identify applicable legal and reporting requirements and issues. Further information specifically related to audits of state and local government entities can be obtained from the National Association of State Auditors, Comptrollers and Treasurers (NASACT).³¹

Under GAGAS, the auditor should design and perform procedures to provide reasonable assurance of detecting instances of violations of legal and regulatory requirements that are significant within the context of the audit objectives. Consequently, if one of the objectives of the audit is to determine whether the entity violated specific laws or regulations, the auditor should plan the audit to detect significant violations of such laws or regulations. In financial audits, the auditor should test those laws and regulations that could have a direct and material effect on the financial statements.

As part of an IS controls audit, the auditor's findings will typically be reported in terms of whether IS controls are effective. While such general laws and regulations as FISMA, FMFIA, FFMIA, and OMB guidance provide requirements and criteria for assessing IS, IS controls audit objectives generally are not focused on detecting violations of such laws and regulations, but rather on assessing controls and identifying any control weaknesses. Consequently, such laws and regulations generally would not be considered significant to the audit objectives for the purposes of designing compliance tests to meet GAGAS. However, audit objectives may

²⁹ OMB, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (Washington, DC: July 12, 2006).

³⁰ OMB, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, M 07-16 (Washington, D.C.: May 22, 2007)

³¹ Intergovernmental Information security Audit Forum, *Information Systems Security Auditing: Legal and Reporting Considerations* (Sept. 11, 2003) www.nasact.org/IISAF/legal.html

Exposure Draft

sometimes include specific objectives to determine compliance with such laws, in which case such laws and regulations would be significant. Also, other laws such as HIPAA, which provide for potential penalties, may be significant to the audit objectives.

2.1.9.B Consideration of the Risk of Fraud

In audits performed under GAGAS, the auditor should assess the risks of fraud³² occurring that is significant within the context of the audit objectives (for financial audits, a material misstatement). Auditors should gather and assess information to identify risks of fraud that are significant within the scope of the audit objectives or that could affect the findings or conclusions. When auditors identify factors or risks related to fraud that has occurred or is likely to have occurred that they believe are significant within the context of the audit objectives, they should design procedures to provide reasonable assurance of detecting such fraud. In financial audits, GAGAS indicates that auditors should assess the risk of material misstatements of financial statement amounts or other financial data significant to the audit objectives due to fraud and to consider that assessment in designing the audit procedures to be performed.³³ The auditor's responsibilities with respect to the risk of fraud in financial statement audits are discussed further in the GAGAS and in the AICPA's Auditing Standards Board Statement on Auditing Standards No. 99, titled *Consideration of Fraud in a Financial Statement Audit*, as amended (AU section 316).

If the IS controls audit is performed as part of a broader financial or performance audit, the auditor should coordinate with the audit team in the identification of and response to the risk of fraud. The auditor should be aware of fraud risks identified by the overall audit team and communicate any fraud risks or suspected fraud associated with IT to the overall audit team. Also, the overall audit

³² Fraud is a type of illegal act involving the obtaining of something of value through willful misrepresentation.

³³ The terms "material" and "significant" are synonymous under generally accepted government auditing standards. In the AICPA standards, "material" is used in relation to audits of financial statements. "Significant" is used in relation to performance audits performed under GAGAS.

Exposure Draft

team may identify audit procedures to be performed by the IS controls specialist to detect fraud significant to the audit.

The audit team should hold a brainstorming session at the start of the audit to discuss potential fraud risks, fraud factors such as individuals' incentives or pressures to commit fraud, the opportunity for fraud to occur, and rationalizations or attitudes that could allow individuals to commit fraud. For example, the following factors related to IS may indicate a risk of fraud:

- failure to provide an adequate security management program, including inadequate monitoring of control effectiveness;
- weaknesses in access and other IS controls that could allow overrides of internal controls or access to systems susceptible to fraud (e.g., payment systems);
- lack of adequate segregation of duties,³⁴ and
- pervasive or long-standing IS control weaknesses.

The auditor should gather and assess information necessary to identify fraud risks that could be relevant to the audit objectives or affect the results of their audit. For example, the auditor may obtain information through discussion with officials of the audited entity or through other means to determine the susceptibility of the program to fraud, the status of internal controls the entity has established to detect and prevent fraud, or the risk that officials of the audited entity could override internal control. The auditor should exercise professional skepticism in assessing these risks to determine which factors or risks could significantly affect the results of their work if fraud has occurred or is likely to have occurred.

When the auditor identifies factors or risks related to fraud that they believe are significant within the context of the audit objectives or the results of the audit, they should design procedures to provide reasonable assurance of detecting such fraud. The auditor should

³⁴ Separation of duties so that no one individual controls all critical stages of a work process. Also see section 3.4 and the definition in the glossary.

Exposure Draft

prepare audit documentation related to their identification and assessment of and response to fraud risks.

Assessing the risk of fraud is an ongoing process throughout the audit and relates not only to planning the audit but also to evaluating evidence obtained during the audit. When testing general and business process application level controls, the auditor should be alert for information or other conditions that indicate fraud that is significant within the context of the audit objectives may have occurred.

A specific area of concern for fraud is override of controls, particularly in ERP applications. Because ERP applications are by their nature highly integrated, the potential risk of management override of controls is heightened. The audit generally should include procedures to identify system-based overrides. These procedures might include testing for instances of users performing inappropriate combinations of transactions (i.e., transactions that should have been segregated) and other similar procedures. Some examples of antifraud controls to consider include: workflow approvals, restricting access to sensitive files, segregation of duties, review of audit trails, and review of key management reports. Access controls, segregation of duties, and audit trails are discussed in Chapter 3.

The auditor should also evaluate situations or transactions that could be indicative of fraud. When information comes to the auditors' attention (through audit procedures, allegations received through fraud hotlines, or other means) indicating that fraud may have occurred, the auditor should evaluate whether the possible fraud could significantly affect the audit results. If the fraud could significantly affect the audit results, auditors should modify the audit steps and procedures, as necessary, to (1) determine if fraud likely has occurred and (2) if so, determine its effect on the audit results.

The auditor's training, experience, and understanding of the program being audited may provide a basis for recognizing that some acts coming to his or her attention may be indicative of fraud. Whether an act is, in fact, fraud is a determination to be made

Exposure Draft

through the judicial or other adjudicative system and is beyond auditors' professional expertise and responsibility. However, the auditor is responsible for being aware of vulnerabilities to fraud associated with the area being audited to identify indications that fraud may have occurred.

2.1.9.C Audit Resources

As with other types of audits, the staff assigned to perform the IS controls audit must collectively possess adequate professional competence. Therefore, it is important to carefully plan IS controls audits to ensure that adequate and appropriate resources are available to perform the audit. IS controls audits need a broad range of technical skills. In addition to skills necessary to assess each control category, IS controls audits generally use technical specialists with skills in such areas as networks, Windows/Novell, Unix, data management systems, and mainframe system and access control software. See Appendix V for a discussion of typical skill sets for IS controls specialists. Based on the knowledge obtained during audit planning, the auditor should identify resource requirements and determine whether internal resources are available or whether contractors will be necessary to complete the audit. The auditor should then schedule the resources for the appropriate periods of time.

Regardless of the size of the entity, the auditor must still perform the necessary planning to ensure that audit requirements are fully satisfied. This includes small/independent agencies which generally have a less complex, less risky IS control environment, which requires inherently fewer IS controls audit resources. The Committee of Sponsoring Organizations (COSO)³⁵ publication "Internal Controls over Financial Reporting – Guidance for Smaller Public Companies" includes guidance that could be used by smaller agencies in planning their audits.

³⁵Is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance.

Exposure Draft

The auditor may determine that it is necessary to contract for audit services for all or a portion of the IS controls audit. For example, the auditor may determine that it is necessary to contract only for certain technical skills needed to perform the audit. Contracting for audit services offers two significant benefits to an entity's audit organization—it allows audit coverage beyond that possible with the existing audit staff level, and it allows the audit activity to address technical and other issues in which the in-house staff is not skilled. Engagements that employ contractors in this way may help train in-house staff for future audits. However, when contracting for audit services, some in-house audit personnel generally should be actively involved. For example, the audit organization should be instrumental in determining the scope of the contracted services, and in developing the task order or request for proposal for the work. The FISCAM may be required to be used as a basis for the work to be performed.

Also, an auditor generally should be designated to monitor the contract for the entity. The contract monitor should have sufficient knowledge of IS controls to monitor and to assess the quality and adequacy of the work performed by the contractor, including the adequacy of the audit documentation. The contract monitor should discuss the contract with the contractor, including the product deliverables, the established time frames for deliverables, and documentation standards to adhere to. The auditor generally should hold this meeting before the contractor begins work. In addition, the contract monitor should attend critical meetings the contractor has with entity representatives, including the opening and close-out meetings.

The contract monitor should conduct a technical review of the work performed and may use this manual as guidance to determine whether the work addressed relevant issues and the audit procedures were adequate. For financial audits, the contract monitor may reperform some tests in accordance with FAM 650, "Using the Reports and Work of Others." Also, the contract monitor should review the audit report and supporting audit documentation to determine whether the audit report is adequately supported.

Exposure Draft

2.1.9.D Multiyear Testing Plans

In circumstances where the auditor regularly performs IS controls audits of the entity (as is done, for example, by an IG or for annual financial audits), the auditor may determine that a multiyear plan for performing IS controls audits is appropriate. Such a plan will cover relevant key agency applications, systems, and processing centers. These strategic plans should cover no more than a 3-year period and include the schedule and scope of assessments to be performed during the period and the rationale for the planned approach. The auditor typically evaluates these plans annually and adjusts them for the results of prior and current audits and significant changes in the IT environment, such as implementation of new systems.

Multiyear testing plans can help to assure that all agency systems and locations are considered in the IS control evaluation process, to consider relative audit risk and prioritization of systems, and to provide sufficient evidence to support an assessment of IS control effectiveness, while helping to reduce annual audit resources under certain conditions. When appropriate, this concept allows the auditor to test computer-related general and business process application controls on a risk basis rather than testing every control every year. Under a multiyear testing plan, different controls are comprehensively tested each year, so that each significant general and business process control is selected for testing at least once during the multiyear period, which should not be more than 3 years. For example, a multiyear testing plan for an entity with five significant business process applications might include comprehensive tests of two or three applications annually, covering all applications in a 2 or 3 year period. For systems with high IS risk, the auditor generally should perform annual testing.

Such multiyear testing plans are not appropriate in all situations. For example, they are not appropriate for first-time audits, for audits where some significant business process applications or general controls have not been tested within a sufficiently recent period (no more than 3 years), or for audits of entities that do not have strong entitywide controls. Also, using this concept, the auditor performs some limited tests and other activities annually for general and business process controls not selected for full testing; examples of such activities include updating the auditor's

Exposure Draft

understanding of the control environment, inquiring about control changes, and conducting walk-throughs. For example, because of the importance of system level critical control points, the auditor generally updates the understanding of these yearly through limited tests. Multiyear testing is discussed in greater detail in FAM section 395 G: “Multiyear Testing of Controls.”

2.1.9.E Communication with Entity Management and Those Charged with Governance

The auditor should communicate information about the audit to appropriate entity management and those charged with governance. The auditor should document this communication, usually with an engagement letter. This step is particularly important in an IS controls audit because of the sensitivity of entity information systems and the nature of tests performed. Multiple meetings may be necessary with various levels of management so that they are adequately aware of the audit process. GAGAS requires that to help the various parties involved in the audit understand the audit objectives, time frames, and any data needs, the auditor should provide them with information about the specific nature of the audit, as well as general information concerning the planning and conduct of the audit and reporting.

As part of this communication, it may be useful to provide general protocols for conducting the IS controls audit. Such protocols might include the following:

- Define the scope of the engagement. This might include an overview of the audit objectives, information about what is to be tested, when testing will occur, where and from what locations testing will be performed, who will be performing and monitoring the testing, and how the testing will be performed (for example, the methodology and tools that will be employed). However, it is important to not disclose detailed audit procedures so that the tests become ineffective.
- Communicate risks and steps taken by management to manage such risks. While risks cannot be eliminated entirely, they can be managed to an acceptable level to avoid, or at least minimize, service degradation or interruption. Auditors can communicate actions they have taken to minimize risks such as (a) not performing denial-of-service testing, (b) coordinating testing with

Exposure Draft

the audited site, (c) having knowledgeable personnel from the audited site monitoring all testing, (d) testing the tools that will be used and gaining expertise in their use, (e) logging test parameters, (f) logging testing and results, (g) using network analyzers to monitor loads placed on the network during testing, and (h) performing testing during nonpeak hours, if possible.

- Identify roles and responsibilities. Address the roles and responsibilities of each participant. Participants will likely include the test team, the auditors, the system owners, the systems security officer, the systems administrators, and contractors, if applicable.
- Address logistical requirements. Logistical requirements would include information about such items as the organization's range of Internet Protocol addresses and telephone numbers (particularly sensitive numbers that should be excluded from testing), analog telephone lines, wireless connections, Internet access paths, policies governing user accounts and passwords, etc. On-site workspace arrangements and agency points of contact might also be addressed.

GAGAS requires certain communications with management, those charged with governance, and others. For financial audits, see AU 380 and GAGAS 4.06. For performance audits, see GAGAS 7.46-7.48. In situations in which those charged with governance are not clearly evident, auditors should document the process followed and conclusions reached for identifying those charged with governance.

2.1.9.F Service Organizations

When IS controls, which are significant to a GAGAS audit, are performed by a service organization external to the audited entity, the auditor should determine how to obtain sufficient, appropriate evidence about the operating effectiveness of such controls. The auditor should coordinate these procedures with the audit procedures performed in support of critical element SM-7 "Ensure That Activities Performed by External Third Parties are Adequately Secure". For example, the auditor should determine how management of the audited entity monitors the effectiveness of IS controls at the service organization, such as through the receipt and analysis of a service auditor (SAS 70) report. SAS 70 reports are

Exposure Draft

discussed in more detail in Appendix VII. If the auditor uses a SAS 70 report, the auditor is responsible for determining whether SAS 70 report provides sufficient evidence about the operating effectiveness of IS controls performed by the service organization that are significant to the audit. Also, see section 2.1.9.G below. If IS controls are performed by service organizations, the auditor should document conclusions whether such controls are significant to the audit objectives and any audit procedures performed with respect to such controls (e.g., review of service auditor reports).

The auditor should integrate evidence obtained about the operating effectiveness of service auditor controls into the IS controls audit. For example, the auditor should evaluate the effectiveness of IS controls for the combination of IS controls at the audited entity and at the service organization collectively. The preparation and use of service auditor reports are discussed further in Appendix VII, including how to determine whether the service auditor report contains sufficient, appropriate evidence.

2.1.9.G Using the Work of Others

The auditor may be able to use the work of the other auditors to support findings or conclusions for the current audit. If auditors use the work of other auditors, they should perform procedures that provide a sufficient basis for using that work. For financial audits, further information on using the work of other auditors is discussed in FAM 650 and AU 336. For performance audits, as discussed in GAGAS 7.41-.43, auditors should obtain evidence concerning the other auditors' qualifications and independence and should determine whether the scope, quality, and timing of the audit work performed by the other auditors is adequate for reliance in the context of the current audit objectives. Procedures that auditors may perform in making this determination include reviewing the other auditors' report, audit plan, or audit documentation, and/or performing tests of the other auditors' work. The nature and extent of evidence needed will depend on the significance of the other auditors' work to the current audit objectives and the extent to which the auditors will use that work.

As discussed in GAGAS 7.43, some performance audits may necessitate the use of specialized techniques or methods that

Exposure Draft

require the skills of a specialist. If auditors intend to use the work of specialists, they should obtain an understanding of the qualifications and independence of the specialists. (See GAGAS paragraph 3.05 for independence considerations when using the work of others.)

Evaluating the professional qualifications of the specialist involves the following:

- a. the professional certification, license, or other recognition of the competence of the specialist in his or her field, as appropriate;
- b. the reputation and standing of the specialist in the views of peers and others familiar with the specialist's capability or performance;
- c. the specialist's experience and previous work in the subject matter; and
- d. the auditors' prior experience in using the specialist's work.

If the auditor plans to use the work of others, the auditor should document conclusions concerning the planned use of the work of others and any audit procedures performed with respect to using the work of others.

2.1.9.H Audit Plan

The auditor should prepare a written audit plan for each audit. The auditor should describe the objectives, scope, and methodology for the IS controls audit. The auditor should include planning information, discussed in the preceding sections of this chapter. If the IS controls audit is a component of a performance audit or attestation engagement, the auditor should integrate such information, as appropriate, into the overall audit plan. If the IS controls audit is a component of a financial audit, the auditor should integrate such information, as appropriate, with the overall audit strategy and audit plan for the financial audit. Additionally, the auditor generally should use the IS controls audit plan as a tool to communicate with the audit team. If the auditor believes that another auditor will use his or her work, the auditor may use the plan to coordinate with the other auditor.

In planning the audit, the auditor generally will first assess the effectiveness of entitywide and system level general controls prior to testing business process application level controls, unless the purpose of the audit is to identify control weaknesses in the

Exposure Draft

application area. Without effective entitywide and system level general controls, business process application level controls may be rendered ineffective by circumvention or modification.

Consequently, if general controls are not designed or operating effectively, the auditor may conclude that assessing business process application level controls is not efficient or necessary to achieve the audit objectives. In such cases, the auditor should develop appropriate findings and consider the nature and extent of risks and their effect on the audit objectives and the nature, timing, and extent of audit procedures. However, if an audit objective is to identify control weaknesses within a business process application, an assessment of the business process application level controls may be appropriate. Also, testing of business process application level controls may be warranted when the auditor finds general control weaknesses mainly in areas with a relatively insignificant impact on business process controls and the key areas of audit interest, but not in more significant areas.

GAGAS require that a written audit plan be prepared for each performance audit. The form and content of the written audit plan may vary among audits and may include an audit strategy, audit program, project plan, audit planning paper, or other appropriate documentation of key decisions about the audit objectives, scope, and methodology and of the auditor's basis for these decisions. The auditor should update the plan, as necessary, to reflect any significant changes to the plan made during the audit. GAGAS include financial audit planning documentation standards.

2.1.10 Documentation of Planning Phase

The auditor should document the following information developed in the planning phase:

- Objectives of the IS auditIS controls audit and, if it is part of a broader audit, a description of how such objectives support the overall audit objectives.
- The scope of the IS auditIS controls audit.
- The auditor's understanding of the entity's operations and key business processes, including, to the extent relevant to the audit objectives, the following:

Exposure Draft

- The significance and nature of the programs and functions supported by information systems;
- Key business processes relevant to the audit objectives, including business rules, transaction flows, and application and software module interaction;
- Significant general support systems and major applications that support each key process;
- Background information request, if used;
- Significant internal and external factors that could affect the IS auditIS controls audit objectives;
- Detailed organization chart, particularly the IT and the IS components;
- Significant changes in the IT environment/architecture or significant applications implemented within the past 2 years or planned within the next 2 years; and
- The entity's reliance on third parties to provide IT services (e.g., in-house, remote connectivity, remote processing).
- A general understanding of the structure of the entity's or component's networks as a basis for planning the IS auditIS controls audit, including high-level and detailed network schematics relevant to the audit objectives.
- Key areas of audit interest, including relevant general support systems and major applications and files. This includes (1) the operational locations of each key system or file, (2) significant components of the associated hardware and software (e.g., firewalls, routers, hosts, operating systems), (3) other significant systems or system-level resources that support the key areas of audit interest, and (4) prior audit problems reported. Also, the auditor should document all access paths in and out of the key areas of audit interest.
- Factors that significantly increase or decrease IS risk and their potential impact on the effectiveness of information system controls. For each risk identified, the auditor should document the nature and extent of the risk; the conditions that gave rise to that risk; and the specific information or operations affected (if not pervasive).
- Preliminary assessment of IS risks related to the key areas of audit interest and the basis for the assessed risk. For each risk

Exposure Draft

identified, the auditor should document the nature and extent of the risk; the conditions that gave rise to that risk; and the specific information or operations affected (if not pervasive). The auditor should also document other considerations that may mitigate the effects of identified risks.

- Critical control points.
- A preliminary understanding of the entity's IS controls, including the organization, staffing, responsibilities, authorities, and resources of the entity's security management function. The auditor should include the following information in the documentation of their preliminary understanding of the design of IS controls, to the extent relevant to the audit objectives:
 - Identification of entitywide level controls (and appropriate system level controls) designed to achieve the control activities for each critical element within each general control area and a determination of whether they are designed effectively and implemented (placed in operation), including identification of control activities for which there are no or ineffective controls at the entitywide level and the related risks;
 - Identification of business process level controls for key applications identified as key areas of audit interest, determination of where those controls are implemented (placed in operation) within the entity's systems, and the auditor's conclusion about whether the controls are designed effectively, including identification of control activities for which there are no or ineffective controls and the related risks and the potential impact of any identified design weaknesses on the completeness, accuracy, validity, and confidentiality of application data;
 - Any internal or third-party information systems reviews, audits, or specialized systems testing (e.g., penetration tests, disaster recovery tests, and application-specific tests) performed during the last year;
 - Management's plans of action and milestones, or their equivalent, that identify corrective actions planned to address known IS weaknessesIS control weaknesses;
 - Status of the prior years' audit findings;

Exposure Draft

- Documentation for any significant computer security related incidents identified and reported for the last year;
- Documented security plans;
- Documented risk assessments for relevant systems (e.g., general support systems and major applications);
- System certification and accreditation documentation or equivalent for relevant systems;
- Documented business continuity of operations plans and disaster recovery plans; and
- A description of the entity's use of third-party IT services
- Relevant laws and regulations and their relation to the audit objectives.
- Description of the auditor's procedures to consider the risk of fraud, any fraud risk factors that the auditor believes could affect the audit objectives, and planned audit procedures to detect any fraud significant to the audit objectives.
- Audit resources planned.
- Current multiyear testing plans.
- Documentation of communications with entity management.
- If IS controls are performed by service organizations, conclusions whether such controls are significant to the audit objectives and any audit procedures performed with respect to such controls (e.g., review of service auditor reports)
- If the auditor plans to use the work of others, conclusions concerning the planned use of the work of others and any audit procedures performed with respect to using the work of others.
- Audit plan that adequately describes the objectives, scope, and methodology of the audit.
- Any decision to reduce testing of IS controls due to the identification of significant IS control weaknesses.

Exposure Draft

2.2 Perform Information System Controls Audit Tests

2.2.1 Overview

In the testing phase of the IS controls audit, the auditor uses information obtained in the planning phase to test the effectiveness of IS controls that are relevant to the audit objectives. As audit evidence is obtained through performing control testing, the auditor should reassess the audit plan and consider whether changes are appropriate.

While determining whether IS controls are appropriately designed and implemented and while performing tests of IS controls, the auditor should periodically assess the cumulative audit evidence obtained to identify any revisions needed to the audit plan. For example, if significant weaknesses have been identified, the auditor may decide to perform less testing in remaining areas if audit objectives have been achieved. Conversely, the performance of tests may uncover additional areas to be tested.

For those IS controls that the auditor determines are properly/suitably designed and implemented, the auditor determines whether to perform tests of the operating effectiveness of such controls. In determining whether to test the operating effectiveness of IS controls, the auditor should determine whether it is possible and practicable to obtain sufficient, appropriate audit evidence without testing IS controls. For federal financial statement audits and for single audits (compliance requirements), the auditor is required to test controls that are suitably designed and implemented to achieve a low assessed level of control risk.

As discussed in Chapter 1, this manual is organized in a hierarchical structure to assist the auditor in performing the IS controls audit. Chapter 3 provides information concerning the general controls, and Chapter 4 provides information concerning four business process application level controls. Each of the chapters contains several control categories, which are groupings of related controls pertaining to similar types of risk. For each control category, this manual discusses the key underlying concepts and associated risks if the controls in the category are ineffective.

Exposure Draft

Chapter 3 is organized by five general control categories:

- security management,
- access controls,
- configuration management,
- segregation of duties, and
- contingency planning.

Chapter 4 is organized into four business process application level control categories:

- business process application level general controls³⁶ (also referred to as application security),
- business process controls,
- interface and conversion controls, and
- data management systems controls.

The last three business process application level control categories are collectively referred to as “business process application controls.”

For each control category, the manual identifies critical elements—tasks that are essential for establishing adequate controls within the category. For each critical element, there is a discussion of the associated objectives, risks, and control activities, as well as related potential control techniques and suggested audit procedures. This hierarchical structure facilitates the auditor’s analysis of identified control weaknesses.

Within each relevant control activity, the auditor should identify control techniques implemented by the entity and determine whether the control techniques, as designed, are sufficient to achieve the control activity. If sufficient, the auditor should determine whether the control techniques are implemented (placed

³⁶ The first category of business process controls is defined as general controls operating at the business process application level.

Exposure Draft

in operation) and are operating effectively. Also, the auditor should evaluate the nature and extent of testing performed by the entity. Such information can assist in identifying key controls and in assessing risk, but the auditor should not rely on testing performed by the entity in lieu of appropriate auditor testing. As discussed later in this section, if the control techniques implemented by the entity, as designed, are not sufficient to address the control activity, or the control techniques are not effectively implemented as designed, the auditor should determine the effect on IS controls and the audit objectives.

The auditor identifies control techniques and determines the effectiveness of controls at each of the following levels:

- Entitywide or component level (general controls) Controls at the entity or component level consist of the entitywide or componentwide processes designed to achieve the control activities. They are focused on how the entity or component manages IS related to each general control activity in Chapter 3. For example, the entity or component may have an entitywide process for configuration management, including establishment of accountability and responsibility for configuration management, broad policies and procedures, development and implementation of monitoring programs, and possibly centralized configuration management tools. The absence of entitywide processes may be a root cause of weak or inconsistent controls, by increasing the risk that IS controls are not applied consistently across the organization.
- System level (general controls) Controls at the system level consist of processes for managing specific system resources related to either a general support system or major application. These controls are more specific than those at the entity or component level and generally relate to a single type of technology. Within the system level are three further levels that the auditor should assess: network, operating system, and infrastructure application. The three sublevels can be defined as follows:
 - *Network*. A network is an interconnected or intersecting configuration or system of components. For example, a

Exposure Draft

computer network allows applications operating on various computers to communicate.

- *Operating system.* An operating system is software that controls the execution of computer programs and may provide various services. For example, an operating system may provide services such as resource allocation, scheduling, input/output control, and data management.
- *Infrastructure applications.* Infrastructure applications are software that is used to assist in performing systems operations, including management of network devices. These applications include databases, e-mail, browsers, plug-ins, utilities, and applications not directly related to business processes. For example, infrastructure applications allow multiple processes running on one or more machines to interact across a network.

For an example of the identification of system level controls, take configuration management. The auditor who is evaluating configuration management at the system level should determine whether the entity has applied appropriate configuration management practices for each significant type of technology (e.g., firewalls, routers) in each of the three sublevels (e.g., specific infrastructure applications). Such configuration management practices typically include standard configuration guidelines for the technology and tools to effectively determine whether the configuration guidelines are effectively implemented.

- Business process application level. Controls at the business process application level consist of policies and procedures for controlling specific business processes. For example, the entity's configuration management should reasonably ensure that all changes to application systems are fully tested and authorized.

Chapter 3 includes general control activities that are applicable to the entitywide and system levels, and Chapter 4 includes the general controls applied at the business process application level (also referred to as application security) as well as the three categories of business process application controls. The control techniques for

Exposure Draft

achieving the control activities and the related audit tests vary according to the level to which they are being applied. However, they are described at a high level in this manual, and these descriptions assume some expertise about the subject to be effectively performed. Thus, the auditor should develop more detailed audit steps based on the entity's specific software and control techniques, after consulting with the financial or performance auditor about audit objectives and significant areas of audit interest. This manual lists specific control activities and techniques and related suggested audit procedures. Table 1 shows the control categories applicable at each level.

Exposure Draft

Table 1: Control Categories Applicable at Different Levels of Audit

	Control Categories	Entitywide/ Component Level	System Level			Business Process Application Level
			Network	Operating Systems	Infrastructure Applications	
General Controls	Security Management					
	Access Controls					
	Configuration Management					
	Segregation of Duties					
	Contingency Planning					
Business Process Application Controls	Business Process Controls					
	Interfaces					
	Data Management Systems					

Source: GAO.

The auditor should evaluate the effectiveness of IS controls including system and/or application level controls related to each critical control point. The auditor should evaluate all potential ways in which the critical control point could be accessed. Generally, for each critical control point, this would include assessing controls

Exposure Draft

related to the network, operating system, and infrastructure application components. For example, if a particular router was deemed to be a critical control point, the auditor generally should test controls related to the router itself (a network component), its operating system, and the infrastructure application that is used to manage the router. Access to any of these could lead to access to the control point. See the discussion of control dependencies in the above section entitled “Identify Critical Control Points”.

As discussed in audit planning (section 2.1.2), the auditor determines the appropriate scope of the IS controls audit, including

- the organizational entities to be addressed (e.g., entitywide, selected component(s), etc.);
- the breadth of the audit (e.g., overall conclusion on IS control effectiveness, review of a specific application or technology area, such as wireless or UNIX, etc.);
- the types of IS controls to be tested:
- general and/or business process application level controls to be tested, or selected components; or
- all levels of the entity’s information systems, or selected levels (e.g., entitywide, system level, or business process application level, or selected components of them).

The auditor should perform the following procedures as part of testing the effectiveness of information system controls:

- Understand information systems relevant to the audit objectives, building on identification of key areas of audit interest and critical control points.
- Determine which IS control techniques are relevant to the audit objectives. The control categories, critical elements, and control activities in Chapters 3 and 4 are generally relevant to all audits. However, if the auditor is not performing a comprehensive audit, for example, an application review, then there may be no need to assess controls in Chapter 3.
- For each relevant IS control technique, determine whether it is suitably designed to achieve the critical activity and has been implemented – placed in operation (if not done earlier).

Exposure Draft

- Perform tests to determine whether such control techniques are operating effectively.
- Identify potential weaknesses in IS controls. For each potential weakness, consider the impact of compensating controls or other factors that mitigate or reduce the risks related to potential weaknesses.

Understand Information Systems Relevant to the Audit Objectives

The auditor should obtain and document an understanding of the information processing steps performed in information systems that are significant to the audit objectives, including:

- The manner in which transactions are initiated;
- The nature and type of records and source documents;
- The processing involved from the initiation of transactions to their final processing, including the nature of computer files and the manner in which they are accessed, updated, and deleted; and
- For financial audits, the process used to prepare the entity's financial statements and budget information, including significant accounting estimates, disclosures, and computerized processing.

This understanding builds on information obtained in audit planning (e.g., identification of key areas of audit interest and critical control points). For efficiency, the auditor may combine this step with audit planning to aid in the identification of relevant controls. The auditor should perform and document walk-throughs for all business process applications that are significant to the audit objectives. Walk-throughs are important for understanding the information processing and for determining appropriate audit procedures.

Identify IS Control Techniques That Are Relevant to the Audit Objectives

Based on the results of audit planning and other procedures performed, the auditor should identify the control categories, critical elements, control activities, and control techniques that are relevant to the IS audit. In doing this, the auditor considers the audit

Exposure Draft

objectives and audit scope, the extent of IS risk and the preliminary understanding of IS controls. The process for identifying relevant control techniques is summarized below.

For IS audits that are stand alone GAGAS audits, generally all of the control categories, critical elements, and control activities are relevant to the audit objectives, unless specifically not part of the audit objectives. For example, in an evaluation of the effectiveness of business process controls in a specific application, the general controls in Chapter 3 may or may not be part of the audit objectives.

At the entitywide level and for each critical control point (including control dependencies) at the system and business process application levels, the auditor should identify and document the control techniques used by the entity to achieve each relevant control activity. For purposes of illustration, using the example of the router serving as a critical control point (as discussed in section 2.1.7), the auditor would identify and document the control techniques used by the entity to achieve the control activities related to each relevant control category and critical element for the router and for the related control dependencies.

If the IS audit is part of a broader financial audit, performance audit, or attestation engagement, the auditor should obtain, from the overall audit team, audit documentation that identifies internal controls that are significant to the audit objectives. For financial audits performed under the FAM, such controls are identified in the SCE form. For each internal control technique that is identified as significant to the audit objectives (significant control technique), the audit team should determine whether it is an IS control. An IS controls specialist generally should review and concur with the audit team's identification of IS controls, particularly with respect to whether all IS controls were properly identified as such.

The auditor should identify and document the other entitywide, system, and business process level IS controls upon which the effectiveness of each significant IS control technique depends. These other IS controls will principally relate to the entitywide level controls and to controls over each of the critical control points (including control dependencies) at the system and business process application levels. For example, if the IS control is the

Exposure Draft

review of an exception report, the auditor should identify and test the business process application controls directly related to the production of the exception report, as well as the general and other business process application controls upon which the reliability of the information in the exception report depends, including the proper functioning of the business process application that generated the exception report and the reliability of the data used to generate the exception report. In addition, the auditor should test the effectiveness of the user control (i.e., management review and followup on the items in the exception report).

For each relevant IS control technique, the auditor should determine whether it is (1) designed effectively to achieve the related control activity, considering IS audit risk and the audit objectives, and (2) implemented (placed in operation). The auditor may be able to determine whether control techniques are sufficient to achieve a particular control activity without evaluating and testing all of the control techniques. Also, depending on IS audit risk and the audit objectives, the nature and extent of control techniques necessary to achieve a particular control objective will vary.

The auditor generally should evaluate the design effectiveness and test only the control techniques necessary to achieve the relevant audit activities. For example, if there are two control techniques, each of which individually would achieve the control activity, the auditor generally would evaluate and test only one control technique. However, if the auditor determines that the control technique evaluated and tested was not effective, the auditor would consider the effectiveness of the other control technique.

Also, the auditor should evaluate the nature and extent of testing performed by the entity. Such information can assist in identifying key controls and in assessing risk, but the auditor should not rely on testing performed by the entity in lieu of appropriate auditor testing. If the control techniques implemented by the entity, as designed, are not sufficient to address the control activity, or the control techniques are not effectively implemented as designed, the auditor should determine the effect on IS controls and the audit objectives.

For efficiency, the auditor may implement a tiered approach to the identification and evaluation of the design effectiveness of relevant

Exposure Draft

IS control techniques, as discussed later in this session, beginning with entitywide level controls, followed by system level controls, then by business process application level controls.

Appendices II and III may be used to identify and summarize relevant IS controls at the entitywide, system, and business process application levels.

Test Information System Controls

The auditor should design and conduct tests of relevant control techniques that are effective in design to determine their effectiveness in operation.

It is generally more efficient for the auditor to test IS controls on a tiered basis, starting with the general controls at the entitywide and system levels, followed by the general controls at the business process application level, and concluding with tests of business process application, interface, and data management system controls at the business process application level. Such a testing strategy may be used because ineffective IS controls at each tier generally preclude effective controls at the subsequent tier.

If the auditor identifies IS controls for testing, the auditor should evaluate the effectiveness of

- general controls at the entitywide and system level;
- general controls at the business process application level; and
- specific business process application controls (business process controls, interface controls, data management system controls), and/or user controls, unless the IS controls that achieve the control objectives are general controls.

The auditor should determine whether entitywide and system level general controls are effectively designed, implemented, and operating effectively by

- identifying applicable general controls;
- determining how those controls function, and whether they have been placed in operation; and
- evaluating and testing the effectiveness of the identified controls.

Exposure Draft

The auditor generally should use knowledge obtained in the planning phase. The auditor should document the understanding of general controls and should conclude whether such controls are effectively designed, placed in operation, and, for those controls tested, operating as intended.

Tests of General Controls at the Entitywide and System Levels

The auditor may test general controls through a combination of procedures, including observation, inquiry, inspection (which includes a review of documentation on systems and procedures), and reperformance using appropriate test software. Although sampling is generally not used to test general controls, the auditor may use sampling to test certain controls, such as those involving approvals.

If general controls at the entitywide and system levels are not effectively designed and operating as intended, the auditor will generally be unable to obtain satisfaction that business process application-level controls are effective. In such instances, the auditor should (1) determine and document the nature and extent of risks resulting from ineffective general controls and (2) identify and test any manual controls that achieve the control objectives that the IS controls were to achieve.

However, if manual controls do not achieve the control objectives, the auditor should determine whether any specific IS controls are designed to achieve the objectives. If not, the auditor should develop appropriate findings principally to provide recommendations to improve internal control. If specific IS controls are designed to achieve the objectives, but are in fact ineffective because of poor general controls, testing would typically not be necessary, except to support findings.

Tests of General Controls at the Business Process Application Level

If the auditor reaches a favorable conclusion on general controls at the entitywide and system levels, the auditor should evaluate and

Exposure Draft

test the effectiveness of general controls for those applications within which business process application controls or user controls are to be tested. These business process application level general controls are referred to as Application Security (AS) controls in Chapter 4.

If general controls are not operating effectively within the business process application, business process application controls and user controls generally will be ineffective. If the IS controls audit is part of a financial or performance audit, the IS controls specialist should discuss the nature and extent of risks resulting from ineffective general controls with the audit team. The auditor should determine whether to proceed with the evaluation of business process application controls and user controls.

Tests of Business Process Application Controls and User Controls

The auditor generally should perform tests of those business process application controls (business process, interface, data management), and user controls necessary to achieve the control objectives where the entitywide, system, and application-level general controls were determined to be effective.

If IS controls are not likely to be effective, the auditor should obtain a sufficient understanding of control risks arising from information systems to

- identify the impact on the audit objectives,
- design audit procedures, and
- develop appropriate findings.

Also, in such circumstances, the auditor considers whether manual controls achieve the control objectives, including manual controls that may mitigate weaknesses in IS controls. If IS controls are not likely to be effective and if manual controls do not achieve the control objectives, the auditor should identify and evaluate any specific IS controls that are designed to achieve the control objectives to develop recommendations for improving internal controls.

Exposure Draft

IS controls that are not effective in design do not need to be tested. If the auditor determined in a prior year that controls in a particular accounting application were ineffective and if management indicates that controls have not significantly improved, the auditor need not test them.

2.2.2 Appropriateness of Control Tests

To assess the operating effectiveness of IS controls, auditors should perform an appropriate mix of audit procedures to obtain sufficient, appropriate evidence to support their conclusions. Such procedures could include the following:

- Inquiries of IT and management personnel can enable the auditor to gather a wide variety of information about the operating effectiveness of control techniques. The auditor should corroborate responses to inquiries with other techniques.
- Questionnaires can be used to obtain information on controls and how they are designed.
- Observation of the operation of controls can be a reliable source of evidence. For example, the auditor may observe the verification of edit checks and password controls. However, observation provides evidence about controls only when the auditor was present. The auditor needs other evidence to be satisfied controls functioned the same way throughout the period.
- The auditor may review documentation of control policies and procedures. For example, the entity may have written policies regarding confidentiality or logical access. Review of documents will allow the auditors to understand and assess the design of controls.
- Inspection of approvals/reviews provides the auditor with evidence that management is performing appropriate control checks. The auditor may combine these tests with discussions and observations.
- Analysis of system information (e.g., configuration settings, access control lists, etc.) obtained through system or specialized software provides the auditor with evidence about actual system configuration.

Exposure Draft

- Data review and analysis of the output of the application processing may provide evidence about the accuracy of processing. For example, a detailed review of the data elements or analytical procedures of the data as a whole may reveal the existence of errors. Computer-assisted audit techniques (CAAT) may be used to test data files to determine whether invalid transactions were identified and corrected by programmed controls. However, the absence of invalid transactions alone is insufficient evidence that the controls effectively operated.
- Reperformance of the control could be used to test the effectiveness of some programmed controls by reapplying the control through the use of test data. For example, the auditor could prepare a file of transactions that contains known errors and determine if the application successfully captures and reports the known errors.

Based on the results of the IS controls audit tests, the auditor should determine whether the control techniques are operating effectively to achieve the control activities. Controls that are not properly designed to achieve the control activities or that are not operating effectively are potential IS control weaknesses. For each potential weakness, the auditor should determine whether there are specific compensating controls or other factors that could mitigate the potential weakness. If the auditor believes that the compensating controls or other factors could adequately mitigate the potential weakness and achieve the control activity, the auditor should obtain evidence that the compensating or other control is effectively operating and actually mitigates the potential weakness. If it effectively mitigates the potential weakness, the auditor can conclude that the control activity is achieved; however, the auditor may communicate such weaknesses to the entity. If the potential weakness is not effectively mitigated, the potential weakness is an actual weakness. The auditor evaluates its effects on IS controls in combination with other identified weaknesses in the reporting phase.

Exposure Draft

2.2.3 Documentation of Control Testing Phase

Information developed in the testing phase that the auditor should document includes the following:

- An understanding of the information systems that are relevant to the audit objectives
- IS Control objectives and activities relevant to the audit objectives
- By level (e.g., entitywide, system, business process application) and system sublevel (e.g., network, operating system, infrastructure applications), a description of control techniques used by the entity to achieve the relevant IS control objectives and activities
- By level and sublevel, specific tests performed, including
 - related documentation that describes the nature, timing, and extent of the tests;
 - evidence of the effective operation of the control techniques or lack thereof (e.g., memos describing procedures and results, output of tools and related analysis);
 - if a control is not achieved, any compensating controls or other factors and the basis for determining whether they are effective;
 - the auditor's conclusions about the effectiveness of the entity's IS controls in achieving the control objective; and
 - for each weakness, whether the weakness is a material weakness, significant deficiency or just a deficiency, as well as the criteria, condition, cause, and effect if necessary to achieve the audit objectives.

Appendices II and III may be used to summarize the results of testing.

Exposure Draft

2.3 Report Audit Results

After completing the testing phase, the auditor summarizes the results of the audit, draws conclusions on the individual and aggregate effect of identified IS control weaknesses on audit risk and audit objectives and reports the results of the audit. The auditor evaluates the individual and aggregate effect of all identified IS control weaknesses on the auditor's conclusions and the audit objectives. The auditor evaluates the effect of any weaknesses on the entity's ability to achieve each of the critical elements in Chapters 3 and 4 and on the risk of unauthorized access to key systems or files. Also, the auditor evaluates potential control dependencies.

For each critical element, the auditor should make a summary determination as to the effectiveness of the entity's related controls, considering entitywide, system, and business process application levels collectively. The auditor should evaluate the effect of related underlying control activities that are not achieved. In addition, the auditor should determine whether the weaknesses preclude the effectiveness of each of the five categories of general controls or the four categories of application-level controls. If the controls for one or more of each category's critical elements are ineffective, then the controls for the entire category are not likely to be effective. The auditor uses professional judgment in making such determinations. For federal entities, if identified weaknesses relate to IS measures reported in FISMA reporting, the auditor should determine whether they were properly reported. Also, the auditor should determine whether IS control weaknesses identified by the audit were identified in the entity's Plans of Action and Milestones (POA&M's) or equivalent document. If not, the auditor generally should attempt to determine why they were not identified by the entity as appropriate and report weaknesses in the reporting process.

Also, the auditor should evaluate whether the aggregate combination of weaknesses could result in unauthorized access to systems or files supporting key areas of audit interest. Guidance for evaluating IS controls and determining the appropriate reporting are

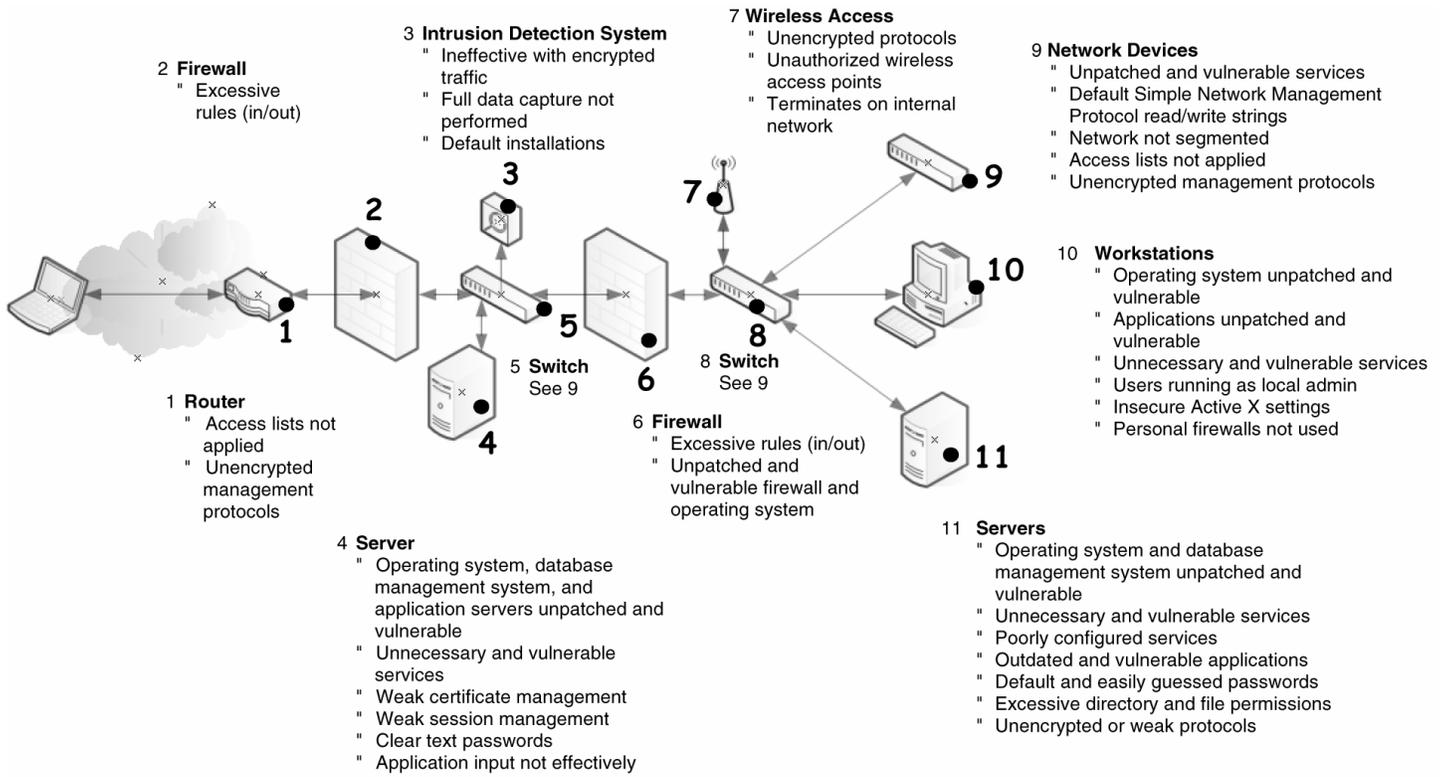
Exposure Draft

discussed separately for financial audits and attestation engagements and for performance audits in the following sections.

For example, a series of weaknesses might result in individuals having the ability to gain unauthorized external access to agency systems, escalate their privileges to obtain a significant level of access to critical control points, and consequently achieve access to key areas of audit interest. The auditor can use simplified network schematics annotated with weaknesses related to key system components to document the impact of a series of weaknesses. Such documentation may be developed as the audit progresses, allowing the auditor to demonstrate on the system that the weaknesses in fact exist and can be exploited to achieve the expected result. Also, such documentation can assist in communicating the related risks to entity management. Figure 3 is an example of a simplified network schematic annotated with weaknesses related to key system components.

Exposure Draft

Figure 3. Example of Network Schematic Describing System Weaknesses



Source: GAO

Further, the auditor should evaluate the potential impact of any identified weaknesses on the completeness, accuracy, validity, and confidentiality of application data relevant to the audit objectives. (See Chapter 4 for a description of completeness, accuracy, validity, and confidentiality.)

When IS controls audits are performed as part of a broader financial or performance audit or attestation engagement, the IS controls specialist should coordinate with the auditor to determine whether significant controls are dependent on IT processing. In very rare circumstances, the auditor may determine that IS controls, in the aggregate, are ineffective, but that the entity has overall compensating controls not dependent on IT processing or that other factors mitigate or reduce the risks arising from IS control weaknesses. For example, manual reviews of support for all disbursements could mitigate certain IS risks related to a

Exposure Draft

disbursement system. If compensating controls or other factors are present, the auditor should document such controls or factors, test them appropriately to determine whether they effectively mitigate the identified IS control weaknesses, and draw conclusions about the nature and extent of the risks that remain after considering such controls or factors.

As noted earlier in the section entitled “Understand the Overall Audit Objectives and Related Scope of the Information System Controls Audit,” if achieving the audit objectives does not require an overall conclusion on IS controls or only relates to certain components of the entity or a subset of controls, the auditor’s assessment would not necessarily identify all significant IS control weaknesses. For example, a limited review of controls over a type of operating system may not identify any significant weaknesses, although there may be very significant weaknesses in other areas that the auditor may not be aware of because of the limited scope of the audit. Consequently, the auditor should evaluate the potential limitations of the auditor’s work on the auditor’s report and the needs and expectations of users. The auditor may determine that, because the limitations are so significant, the auditor (1) will communicate the limitations to the audited entity, those charged with governance, and those requesting the audit and (2) clearly report such limitations on the conclusions in the audit report. For example, in reporting on an audit of an operating system, the auditor may determine that it is appropriate to clearly report that the scope of the assessment was limited to the operating system and that, consequently, additional IS control weaknesses may exist that could impact the effectiveness of IS controls related to the operating system and to the entity as a whole.

The auditor should express the effect of identified IS control weaknesses in terms of the audit objectives. The following sections provide guidelines for assessing IS controls in financial and performance audits. For financial audits and attestation engagements, GAGAS states that auditors should report material weaknesses and other significant deficiencies.

Exposure Draft

2.3.1 Financial Audits and Attestation Engagements

The auditor should conclude whether IS control weaknesses, individually or in the aggregate, constitute a significant deficiency or material weakness in financial reporting. The auditor should coordinate these procedures with the overall audit team. For financial audits, GAGAS and OMB Circular A-123 state that a control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that even if the control operates as designed, the control objective is not always met. A deficiency in operation exists when a properly designed control does not operate as designed or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively. In addition, in financial audits of federal entities, the auditor should evaluate the effect of IS control weaknesses on FFMIA and FMFIA reporting.

GAGAS uses the following definitions and guidelines for classifying internal control weaknesses:

A **significant deficiency** is a deficiency in internal control, or combination of deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood³⁷ that a

³⁷The term "more than remote" used in the definitions for significant deficiency and material weakness means "at least reasonably possible." The following definitions apply: (1) Remote—The chance of the future events occurring is slight. (2) Reasonably possible—The chance of the future events or their occurrence is more than remote but less than likely. (3) Probable—The future events are likely to occur.

Exposure Draft

misstatement of the entity's financial statements that is more than inconsequential³⁸ will not be prevented or detected.

A **material weakness** is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

OMB Circular A-123 uses the same definition for significant deficiency, but continues to refer to it as a reportable condition.

In determining whether IS control deficiencies, individually or in the aggregate, constitute a significant deficiency or material weakness, the auditor should evaluate several factors, including the following:

- The likelihood that an individual could obtain unauthorized access to or perform unauthorized or inappropriate activities on key entity systems or files that could affect information recorded in the financial statements. This might include (1) the ability to obtain root access to systems that house key financial systems (including feeder systems), thereby enabling unauthorized users to read, add, delete, or modify financial data either directly or through the introduction of unauthorized software; (2) the ability to directly access and modify files containing financial information; or (3) the ability to assign unauthorized application user rights, thereby entering unauthorized transactions.
- The nature of unauthorized access that could be obtained (e.g., limited to system or application programmers or system administrators; all authorized system users; or anyone through unauthorized external access through the Internet) or the nature

³⁸ The phrase "more than inconsequential" as used in the definition of significant deficiency describes the magnitude of potential misstatement that could occur as a result of a significant deficiency and serves as a threshold for evaluating whether a control deficiency or combination of control deficiencies is a significant deficiency. A misstatement is "inconsequential" if a reasonable person would conclude, after considering the possibility of further undetected misstatements, that the misstatement, either individually or when aggregated with other misstatements, would clearly be immaterial to the financial statements. If a reasonable person would not reach such a conclusion regarding a particular misstatement, that misstatement is more than inconsequential.

Exposure Draft

of unauthorized or inappropriate activity that could be performed.

- The likelihood that financial statement amounts could be materially affected.
- The likelihood that other controls including business process application controls would prevent or detect such unauthorized access. Generally, if the effectiveness of such other controls depends on computer processed information, it is unlikely that they could effectively prevent or detect such access, unless the identified IS control weaknesses could not reasonably result in the ability to compromise such other controls.
- The risk that management could override controls (such as through excessive access rights).

Based upon these considerations, the auditor should determine whether IS control deficiencies, individually or in the aggregate, are a material weakness or significant deficiency. Also, the auditor should evaluate whether significant deficiencies, in combination, result in material weaknesses. If so, the auditor should determine them to be material weaknesses in drawing conclusions as to the effectiveness of internal control and reporting findings, as discussed in FAM paragraphs 580.42–.48 and 580.51–.58. If the control deficiencies constitute a material weakness, the auditor should conclude that internal controls are not effective.

Financial auditors may take one of two different approaches to reporting on internal control: (1) express an opinion on internal control (see FAM paragraphs 580.38–.48) or (2) report weaknesses found, categorized as material weaknesses or other significant deficiencies, but do not give an opinion (see FAM paragraphs 580.49–.50). GAO auditors generally express an opinion on internal control. In either case, the auditor considers whether internal control is sufficient to meet the following control objectives insofar as those objectives pertain to preventing or detecting misstatements, losses, or noncompliance that would be material in relation to the financial statements:

- Reliability of financial reporting—transactions are properly recorded, processed, and summarized to permit the preparation

Exposure Draft

of the financial statements and supplemental information in accordance with Generally Accepted Accounting Principles (GAAP), and assets are safeguarded against loss from unauthorized acquisition, use, or disposition.

- Compliance with applicable laws and regulations—transactions are executed in accordance with laws governing the use of budget authority; other laws and regulations that could have a direct and material effect on the financial statements or required supplementary information (RSI); and any other laws, regulations, and governmentwide policies identified by OMB in its audit guidance.

The auditor may report weaknesses that do not meet the criteria for significant deficiencies in a letter to management or orally to an appropriate level of the entity. The auditor may include suggestions for corrective action for these less significant weaknesses if enough is understood about their cause. (More detailed information on how and where to report control weaknesses for financial statement audits is presented in sections 580.48 through 580.52 of the FAM.)

2.3.2 Performance Audits

The auditor should draw conclusions on the effectiveness of IS controls relevant to the audit objectives. Depending on the audit objectives, the auditor's report will vary. For example, the auditor's report may

- provide an overall conclusion (e.g., the entity's IS controls are or are not effective in achieving the IS control objectives relevant to the audit) and communicate identified weaknesses;
- limit reporting to identified weaknesses without providing an overall conclusion (e.g., "based on our work, we identified the following IS control weaknesses"); or
- if in support of a broader performance audit, report findings in the context of the audit objectives, such as how they relate to the assessment of the reliability of computer-processed data.

Exposure Draft

GAGAS state that auditors should include in their audit reports the scope of their work on internal control (which includes IS controls) and any deficiencies in internal control that are significant within the context of the audit objectives and based upon the audit work performed. Determining whether and how to communicate to officials of the audited entity internal control deficiencies that have an inconsequential effect on the financial statement or subject matter is a matter of professional judgment. Auditors should document such communications. The auditor may report such inconsequential weaknesses orally to officials of the entity or in a separate written communication.

In determining the significance of the IS control weaknesses, the auditor should evaluate several factors, including the following:

- The likelihood that an individual could obtain unauthorized access to or perform unauthorized or inappropriate activities on key entity systems or files that could affect key areas of audit interest. This might include (1) the ability to obtain root access to systems that house key areas of audit interest (including supporting systems), thereby enabling an intruder to read, add, delete, or modify data either directly or through the introduction of unauthorized software; (2) the ability to directly access and modify files related to key areas of audit interest; or (3) the ability to assign unauthorized application user rights, thereby enabling an intruder to enter unauthorized transactions or perform unauthorized activities.
- The nature of unauthorized access that could be obtained (e.g., limited to system or application programmers or system administrators; authorized system users; or anyone through unauthorized external access through the Internet)
- The likelihood that the achievement of the audit objectives would be significantly affected.
- The likelihood that other controls including business process application controls would prevent or detect such unauthorized access. Generally, if the effectiveness of such other controls depends on computer processed information, it is unlikely that they could effectively prevent or detect such access, unless the identified IS control weaknesses could not reasonably result in the ability to compromise such other controls.

Exposure Draft

- The risk that management could override controls (such as through excessive access rights).
-

2.3.3 Other Audit Reporting Considerations

It is important to report IS control weaknesses in terms that are understandable to individuals who may have limited expertise regarding information systems issues. In this regard, the auditor generally should define technical terms and avoid jargon and undefined abbreviations and acronyms.

Auditors should develop the elements of the findings to the extent necessary to achieve the audit objectives. The extent to which the auditor should develop the elements for a finding (criteria, condition, cause, and effect) depends on the audit objectives. If auditors are able to sufficiently develop the findings, they should provide recommendations for corrective action if they are significant within the context of the audit objectives.

Criteria describe the required or desired state, or what is expected from the program or operation. Condition is the actual situation. Cause is the factor or factors responsible for the difference between condition and criteria. Effect is the impact of the difference between the condition and the criteria. This information helps senior management understand the significance of the weakness and develop appropriate corrective actions. For most types of IS control weaknesses, this manual includes a discussion of risks and potential negative effects that can be adapted for audit reports. GAO has issued numerous reports that can be used as models for reporting computer-related weaknesses. Current IS reports can be obtained from GAO's report database on GAO's Web site (<http://www.gao.gov>).

In many cases, auditors will have detailed information on control weaknesses that is too technical to be meaningful to most senior managers and other users of the audit report, but may be valuable to the audit report, but that may be valuable to the entity's technical staff in understanding the precise cause of the weaknesses and in developing corrective actions. The auditors generally should provide this information to the entity's technical staff in briefings. The

Exposure Draft

auditor should provide information to technical staff that is in substance the same as that reported to senior management.

The auditor should effectively communicate the results of an IS controls audit to the appropriate persons through appropriate reports. This serves several purposes, including

- informing the audited entity and those charged with governance of control weaknesses; issues of noncompliance with laws, regulations, and provisions of contracts or grant agreements; and instances of fraud, illegal acts, or abuse;
- providing the audited entity with recommendations to correct such control weaknesses;
- providing the financial or performance auditor an understanding of the information systems control environment and the effects of IT on the processing of transactions;
- complying with legal reporting requirements; and
- complying with auditing standards, including generally accepted government auditing standards.

However, the auditor should avoid the disclosure of sensitive IS data. An individual could potentially compromise a system from any location in the world, as long as they have access to a computer and a telephone line or Internet connection. Technical information discussed in an audit report could potentially assist individuals by reducing the time and effort to obtain unauthorized access and compromise a system. Also, to avoid disclosure of sensitive information, the auditor should provide draft IS reports to the entity for a sensitivity review. The auditor should evaluate entity sensitivity concerns and make appropriate report revisions, considering legal or regulatory requirements, including the exercise of information classification authority.

Generally, in the federal environment, either one report with limited distribution or two reports, one of which has limited distribution, are issued. Information systems security audit reports may or may not be put on agency Web sites or released under FOIA, generally depending on the degree or extensiveness of sensitive data. Even though these reports may not be posted on agency Web sites, they

Exposure Draft

are still typically issued to agency management. Also, state laws and regulations may affect the form of reporting. For further information, see *Information Systems Security Auditing: Legal and Reporting Considerations*.³⁹

2.3.4 Related Reporting Responsibilities

In addition to reporting the results of the audit, the auditor may have other related reporting responsibilities established by law, regulation, or policy. The auditor should identify any other reporting requirements and respond appropriately.

In financial audits of federal entities, the auditor should determine whether the IS control weaknesses, individually or in the aggregate, constitute a material weakness for FMFIA reporting or a lack of substantial compliance of the entity's systems with FFMIA. See FAM 260.53-57 for further information. Also, further information about reporting IS control weaknesses in relation to a financial audit are discussed in FAM 580 (Draft Reports).

OMB Circular A-123 provides requirements for complying with FMFIA. The Circular requires management to assess controls and provide an annual assurance statement on the overall adequacy and effectiveness of internal control within the agency. In addition, management is required to provide a separate assurance statement on the effectiveness of internal control over financial reporting, which includes safeguarding of assets and compliance with applicable laws and regulations. Also, OMB audit guidance requires management to include representations about internal control in its management representation letter to the auditor.

FMFIA requires agencies to evaluate and report on the adequacy of the systems of internal accounting and administrative control. For the *overall assessment* of internal control, OMB Circular A-123 defines a **material weakness** as a reportable condition which the agency head determines to be significant enough to report outside

³⁹ Intergovernmental Information Security Audit Forum (Sept. 11, 2003); see www.nasact.org

Exposure Draft

of the agency. It defines a **reportable condition** as a control deficiency, or combination of control deficiencies, that in management's judgment, should be communicated because they represent significant weaknesses in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives. For the *assessment of internal control over financial reporting*, Circular A-123 uses the same definitions for material weakness and significant deficiency described above for financial audits, except that OMB uses the term reportable condition rather than the term significant deficiency. Also, FMFIA and OMB Circular A-123 require management to report nonconformances with system requirements. The Circular defines nonconformances as instances in which financial management systems do not substantially conform to financial systems requirements. Financial management systems include both financial and financially-related (or mixed) systems.

The auditor should evaluate the material weaknesses reported under FMFIA to determine whether they meet the definitions of material weakness and reportable condition for reporting as part of management's assertion about the effectiveness of internal control.

FISMA requires federal agencies to report significant deficiencies in IS as material weaknesses under FMFIA and, if relating to financial management systems, as an instance of a lack of substantial compliance of systems with FFMA. The term "significant deficiency" used in FISMA differs from the same term used in GAGAS. OMB defines a FISMA significant deficiency as "a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken." The following points provide guidance in determining whether there is a FISMA significant deficiency:

Exposure Draft

- If IS controls are ineffective with respect to one of the nine control categories (see table 1), such ineffective control(s) represent a FISMA significant deficiency.
- If IS controls are ineffective with respect to one or more critical elements (that is, tasks that are essential for establishing adequate controls within a given control category; examples are given in Chapters 3 and 4), such ineffective control(s) represent a FISMA significant deficiency unless, based upon the facts and circumstances, other factors sufficiently mitigate the effect of the control weaknesses.
- If individual weaknesses meet the above definition, such ineffective control(s) represent FISMA significant deficiencies.

FFMIA requires agencies to implement and maintain financial management systems that comply substantially with federal financial management systems requirements, applicable federal accounting standards, and the U.S. Government Standard General Ledger⁴⁰ at the transaction level. FFMIA requires auditors to assess whether an agency's financial management systems comply with system requirements. IS control weaknesses are a major concern for federal agencies and the general public and are one of the frequently cited reasons for noncompliance with FFMIA.

2.3.5 Documentation of Reporting Phase

The auditor should document appropriate IS information developed in the reporting phase, including:

- The auditor's conclusion about the effectiveness of IS controls (in relation to the IS controls audit objectives) in achieving the critical elements and the relevant control activities and the basis for the conclusion, including the factors that the auditor considered in making the determination

⁴⁰ The *U.S. Government Standard General Ledger* (SGL) provides a uniform chart of accounts and pro forma transactions used to standardize federal agencies' financial information accumulation and processing throughout the year, enhance financial control, and support budget and external reporting, including financial statement preparation.

Exposure Draft

- If part of a broader audit, the impact of any identified IS control weaknesses on the overall audit objectives
- Copies of any reports or written communications issued in connection with the audit, including the draft the agency commented on and entity management comments related to such reports and communications
- For financial audits and attestation engagements, the auditor's determination of whether identified weaknesses represent material weaknesses or significant deficiencies, and the basis for the auditor's conclusions
- Other documentation required by the audit organization's policies and procedures, including quality assurance processes
- Results of procedures to detect any fraud significant to the audit objectives and the impact on the audit
- Results of audit follow-up procedures to determine whether agency corrective actions have been implemented, to sufficiently remediate previously reported IS control weaknesses
- As appropriate, the auditor's considerations and determinations concerning FMFIA, FFMLA, and other reporting responsibilities

2.4 Documentation

The auditor should adequately document the IS controls audit. GAGAS has general documentation requirements for financial and performance audits and attestation engagements. In summary, they are as follows:

Financial Audits - Auditors must prepare audit documentation in connection with each engagement in sufficient detail to provide a clear understanding of the work performed (including the nature, timing, extent, and results of audit procedures performed), the audit evidence obtained and its source, and the conclusions reached. Auditors should prepare audit documentation that enables an experienced auditor, having no previous connection to the audit, to understand **a.** the nature, timing, and extent of auditing procedures performed to comply with GAGAS and other applicable standards and requirements; **b.** the results of the audit procedures performed and the audit evidence obtained; **c.** the conclusions reached on

Exposure Draft

significant matters; and **d.** that the accounting records agree or reconcile with the audited financial statements or other audited information.

Attestation Engagements - Auditors must prepare attest documentation in connection with each engagement in sufficient detail to provide a clear understanding of the work performed (including the nature, timing, extent, and results of attest procedures performed); the evidence obtained and its source; and the conclusions reached. Auditors should prepare attest documentation in sufficient detail to enable an experienced auditor, having no previous connection to the attestation engagement, to understand from the documentation the nature, timing, extent, and results of procedures performed and the evidence obtained and its source and the conclusions reached, including evidence that supports the auditors' significant judgments and conclusions. Auditors should prepare documentation that contains support for findings, conclusions, and recommendations before they issue their report.

Auditors also should document the following for attestation engagements performed under GAGAS: **a.** the objectives, scope, and methodology of the attestation engagement; **b.** the work performed to support significant judgments and conclusions, including descriptions of transactions and records examined; **c.** evidence of supervisory review, before the attest report is issued, of the work performed that supports findings, conclusions, and recommendations contained in the attest report; and **d.** the auditors' consideration that the planned procedures are designed to achieve objectives of the attestation engagement when (1) evidence obtained is dependent on computerized information systems, (2) such evidence is material to the objective of the engagement, and (3) the auditors are not relying on the effectiveness of internal control over those computerized systems that produced the evidence. Auditors should document (1) the rationale for determining the nature, timing, and extent of planned procedures; (2) the kinds and competence of available evidence produced outside a computerized information system, or plans for direct testing of data produced from a computerized information system; and (3) the effect on the attestation engagement report if evidence

Exposure Draft

to be gathered does not afford a reasonable basis for achieving the objectives of the engagement.

Performance Audits – Auditors must prepare audit documentation related to planning, conducting, and reporting for each audit. Auditors should prepare audit documentation in sufficient detail to enable an experienced auditor, having no previous connection to the audit, to understand from the audit documentation the nature, timing, extent, and results of audit procedures performed, the audit evidence obtained and its source and the conclusions reached, including evidence that supports the auditors’ significant judgments and conclusions. Auditors should prepare audit documentation that contains support for findings, conclusions, and recommendations before they issue their report. Auditors should document the following: **a.** the objectives, scope, and methodology of the audit; **b.** the work performed to support significant judgments and conclusions, including descriptions of transactions and records examined; and **c.** evidence of supervisory review, before the audit report is issued, of the work performed that supports findings, conclusions, and recommendations contained in the audit report.

In addition to meeting these general requirements, the auditor should include, in IS controls audit documentation, the specific information discussed throughout this chapter, and summarized in Appendix XI.

2.5 Other Information System Controls Audit Considerations

In addition to the above, the auditor should apply the following topics and techniques to the extent they are relevant to the entity, the audit objectives, and the audit procedures.

- Additional IS risk factors
- Automated audit tools
- Sampling techniques

Also, guidance is provided to the auditor in the evaluation of IS controls associated with service organizations, single audits, and

Exposure Draft

FISMA independent evaluations. Guidance on each of these areas is included in Appendix VII, VIII, and IX, respectively.

2.5.1 Additional IS Risk Factors

As part of the risk assessment, the auditor should also evaluate the following additional IS risk factors to the extent that they are relevant to the entity and the audit objectives. The auditor's risk assessment also includes other risk factors not listed here (e.g., Voice over Internet Protocol – VoIP)

2.5.1.A Defense-In-Depth Strategy

Defense-in-Depth is a commonly accepted “best practice” for implementing computer security controls in today's networked environments. In some agencies, the auditor may encounter this strategy as part of the agency's security management program. Where an effective Defense-in-Depth strategy has been implemented by the entity, the auditor's assessment of IS risk would generally be lower. Conversely, where this strategy is not used, the auditor's assessment of IS risk would generally be higher. The auditor's IS control testing generally provides evidence about the effectiveness of a Defense-in-Depth strategy. See Chapter 3 (AC-1 and CM-5) for additional information on Defense-in-Depth strategy.

According to the National Security Agency, Defense-in-Depth integrates people, operations, and technology capabilities to protect information systems across multiple layers and dimensions. For example, successive layers of defense will cause an adversary who penetrates or breaks down one barrier to promptly encounter successive barriers until the attack ends. The strategy recommends a balance between protection capabilities and cost, performance, and operational considerations.

The people component of Defense-in-Depth begins with a senior-level management commitment (normally at the chief information officer level) that is based on a clear understanding of the perceived threat. This component must be implemented with effective information security policies and procedures, assignment of roles and responsibilities, commitment of resources, training and awareness programs (for both users and system administrators),

Exposure Draft

and personnel accountability, which includes the establishment of physical and personnel security measures to control and monitor access to facilities and critical elements of the information technology environment.

The operations component focuses on all activities required to sustain an agency's security posture on a day-to-day basis. These activities include

- maintaining up-to-date system security policies,
- establishing certification and accreditation programs,
- managing information system security (for example, installing patches and virus updates, maintaining access control lists),
- performing system security assessments (for example, vulnerability assessments),
- auditing and monitoring system activity and responding to threats, and
- implementing recovery and reconstitution procedures in the event of a security breach.

The technology component includes defense in multiple places and layered defense mechanisms that provide intrusion prevention, detection, and response to security incidents. Since attackers may target multiple points in an information system, an agency needs to deploy protection mechanisms at multiple locations including the protection of local and wide area communication networks (for example, from denial of service attacks), protection for data transmitted over the networks (for example, use of encryption and traffic flow security measures), defense of enclave boundaries (for example, deploy firewalls and intrusion detection systems), and defense of the computing environment (for example, access control on hosts and servers). Even the best security products have inherent weaknesses, so it is only a matter of time before an attacker finds an exploitable vulnerability. Therefore, it is important to deploy layered defense mechanisms such as nested firewalls coupled with intrusion detection at outer and inner network boundaries, between the adversary and the target.

Exposure Draft

2.5.1.B Web Applications

Web applications, which use a web browser as part of the application, present significant additional IS risks because, if not properly controlled, they can expose the application and the entity's systems to unauthorized access. In some instances, the risk related to the application itself may be low because it is not critical or it does not contain sensitive information. However, if not properly controlled, it could be used to obtain unauthorized access to other entity system resources. Therefore, due to the heightened risk, even if a web application itself is not part of the scope of the audit, the auditor should assess the effectiveness of web application security and, as appropriate, general controls to determine whether the information system controls over the application could allow unauthorized access through the application to other system resources.

2.5.1.C ERP Systems

ERP systems present additional IS risks. While IS control objectives contained in the FISCAM, if properly achieved, should address such risks, it is important for the auditor to properly consider how the control objectives are achieved in ERP systems. This section provides some considerations in auditing ERP systems. The auditor should supplement the FISCAM with audit considerations and techniques that are specific to the particular ERP system(s) being audited. Although ERP systems share some similar functionality, the way they are implemented and the audit techniques (e.g., specific system queries, analysis of superuser capabilities) applied will vary with the particular vendor.

Factors affecting the overall risk related to ERP systems include the following:

- ERP systems are highly integrated (e.g., common databases, common security administration) and cover/include/address a broad range of entity activities, which leads to increased risks related to several control areas. For example, an ERP application generally includes a broader cross-section of users in the entity, increasing the need for access (particularly least privilege) and segregation of duties controls. Also, because loss of an ERP system/application can have devastating consequences to an

Exposure Draft

entity, the entity needs effective controls over (1) system development/configuration management controls to provide reasonable assurance that the system will operate as intended, (2) service continuity/contingency planning to recover the more comprehensive ERP systems, and (3) access and other general controls to prevent unauthorized access to entity system resources that could lead to denial of service. Further, general controls over the ERP system and supporting databases and operating systems are important to adequately protect access to the underlying data and processing.

- Because ERP systems are on-line-real-time systems, data validation controls are critical to reasonably assure that only valid data is processed by the ERP systems. Controls in ERP systems tend to be preventive rather than detective, as subsequent detection and correction of errors may be costly or impossible. Also, fewer controls may be in place as the data is generally entered and validated once.
- The network architectures for ERP systems are typically more distributed, resulting in increased access controls and other risks than for more centralized systems.
- Because security administration is generally centralized and powerful access is provided to system administrators, access controls over security administration and segregation of duties controls are important. In addition, ERP systems have powerful default user IDs that need to be adequately controlled.
- The broader number of users may also lead to an increase in external access (wireless or other remote access), from both a broader range of internal users as well as external users (e.g., vendors, customers), increasing the number of access points to the entity's systems.
- ERP systems typically have limited, if any, paper audit trails. Consequently, controls over audit logs and other general controls are important for the reliability of data in the ERP systems. Also, auditing access to ERP systems is typically performed online.
- In many instances, interfaces are developed between the ERP system and legacy applications. As a result, the adequacy of interface controls and configuration management controls are important to ensure that data from legacy systems is reliable,

Exposure Draft

valid, complete, and properly converted from the legacy application into the ERP system.

- ERP systems may have a program change control module that allows for direct changes to production code. Therefore, controls related to segregation of development, test and production facilities and functions may not be present. Consequently, IS risks related to configuration management and monitoring are increased, and the entity should secure and monitor such modules.

ERP systems contain certain controls that are not changeable by the entity. It is important to understand these controls and how they may help to achieve the IS control objectives.

In addition, due to the increased risks discussed above, there are a number of other controls that are of increased significance in ERP systems, including controls relating to:

- user access to sensitive application capabilities (e.g., pages, screens, transactions, menus, queries), including related segregation of duties
- powerful user roles/profiles, including defaults
- default user IDs and default passwords
- default system configurations
- access to critical tables/databases
- access to log files
- the effectiveness of the settings of configurable controls
- sensitive reports/outputs

2.5.1.D Interface Controls

Interface controls are particularly important when applications rely on input from legacy systems. Such legacy systems are sometimes referred to as feeder systems. In certain instances, such legacy applications may not have been designed to fully achieve the objectives of the application they support. Consequently, the auditor evaluates the adequacy of interface controls and of application controls related to such legacy applications to provide reasonable assurance that data from legacy systems is reliable, valid, complete, and properly converted from the legacy applications into the

Exposure Draft

applications they support. In addition, the auditor should assess the effectiveness of application controls over the legacy applications, if the reliability of input is relevant to the audit objectives.

2.5.1.E Database Management Systems

Operational characteristics of various system architectures that include Database Management Systems (DBMS) software introduce several potential vulnerabilities to the data/application the DBMS directly supports and the general controls environment, itself. The degree to which these potential vulnerabilities increase risk is determined by the characteristics of the networks and host system(s) involved. One area of risk exists when the DBMS architecture involves multiple installations of the DBMS, which may be located on more than one host system. System and/or application architectures that utilize multiple DBMS installations are commonly used to support functionally or geographically distributed operations, high performance requirements, high availability requirements or some combination of these factors. When multiple DBMSs exist, the mechanisms that allow them to communicate with each other need to be implemented and controlled to prevent unintended data and/or system access. Additionally, modern DBMS software contains powerful capabilities to access the host's operating system and other operating systems and other DBMSs across networks. The ability to use these capabilities needs to be carefully controlled for each DBMS installation. Finally, some administrator accounts in DBMS software provide privileged levels of access to the host's operating system. So, users with system administration privileges in DBMS software may also have significant privileges in host operating systems and those systems and network devices accessible from the DBMS's host.

2.5.1.F Network-based Access Control Systems

Implementations of network-based access control systems (such as LDAPs, including the Microsoft Active Directory™) introduce the potential for specific vulnerabilities. Network-based access control systems are typically hosted on one or more server-class systems. The appropriate configuration of the operating systems and all factors that can effect the functioning of the operating systems for these hosts needs to be carefully controlled. A flaw in operating

Exposure Draft

system-level controls on these hosts potentially jeopardizes the reliability of the control functions provided by the network-based access control system and/or the sensitive access control data contained in that system. Network-based access control systems are designed to support high performance and simplify network administration and maintenance. To facilitate these design considerations, the systems provide flexible methods to connect to and transfer information with other systems. Due to these characteristics, it is essential that effective controls be in place to prevent unintended system functions or data access that could compromise access controls. The nature of networks and application architectures that employ network-based access control systems involves a shared or common reliance on them for critical controls. Therefore, a compromise of a network-based access control system has the potential of contributing to the compromise of other systems.

2.5.1.G Workstations

In modern systems best described as networks of networks, the effect of workstation controls can be much more significant than control over the functions nominally identified as associated with a specific workstation. Workstations can become critical components of a network's perimeter as a result of the manner in which they are configured in the network, the types of sessions they can create with other devices, the access privileges allowed to workstation users, software running on those workstations, and controls over both inbound and outbound network traffic to and from the workstation. An understanding of the configuration of controls on workstations and network-based controls over workstations in the context of network perimeter controls is necessary to assess risk for any network,

2.5.2 Automated Audit Tools

Various automated audit tools can be used to improve the effectiveness and efficiency of the IS controls audit. Sometimes referred to as CAATs, or computer-assisted audit techniques, such tools may be used by the auditor to gather, or assist in gathering,

Exposure Draft

audit evidence. If the auditor plans to use automated audit tools, the auditor should understand

- when they could be used,
- how they can be used, and
- the associated risks.

In addition, the auditor should be adequately trained in the use/operation of these tools and in the interpretation of the results. Because some tools generate a significant volume of information, the auditor should understand how to analyze such information.

Also, the auditor should obtain reasonable assurance that the tools and their use/application produce reliable results and present a reasonably low risk of disrupting the entity's systems. Organizations should develop a process to select, evaluate, and revise software security tools. The following are some typical steps:

- Research available security tools, listing several in each category.
- Discuss with other members of your audit organization which tools could be most useful in-house and at sites to be audited. Discuss with other audit organizations as appropriate.
- Determine the degree of platform-specific security software needed.
- Determine a methodology to evaluate and select software.
- Develop a procedure to train personnel in its use.
- Develop a review process to determine whether the software tool has produced results commensurate with its cost.

There are many different types of automated audit tools:

- Commercial software, such as Microsoft Excel™, etc., may be used by the auditor for analyzing data imported from client files, writing audit programs, etc.
- Generalized audit software may be used by the auditor to query and extract information from the entity's information system. For example, data extraction tools and reporting facilities for access control software can identify users with excess privileges that

Exposure Draft

circumvent segregation of duties. IDEA is the generalized software package available to GAO auditors.

- An embedded audit module is a CAAT in which code prepared by the auditor is embedded in the client's software to replicate a specific aspect of a control procedure, or to record details of certain transactions in a file accessible only to the auditor.
- An integrated test facility is testing software that is integrated into the client's software and enables the auditor's test data to be integrated and processed with the client's live input.
- Using an integrated test facility allows the auditor to be satisfied that test data are processed in the same way that live data are processed and to verify that the results are correct. Parallel simulation is a technique in which actual client data are processed by a copy of the client's software that is under separate control of the auditor and has undergone program code analysis to ensure that the processing is identical to that of the client's operational software.
- Program code analysis is the analysis of the client's program code to ensure that the instructions given to the computer are the same instructions that the auditor has previously identified when reviewing the systems documentation.
- A test data CAAT is a technique in which test data prepared by the auditor are processed on the current production version of the client's software, but separately from the client's normal input data. Using the current production software provides evidence that the transactions were processed in the manner expected.
- Specialized audit software is software designed to perform specific tasks in specific circumstances, such as comparison of source and object code, the analysis of unexecuted code, and the generation of test data.
- Other specialized tools can be used to test IS controls. For example:
 - Password crackers can identify the use of vendor-default or easily guessed passwords.
 - Network "sniffers" (software that can intercept and log traffic passing over a network) can identify the transmission of passwords or sensitive information in clear text.

Exposure Draft

- Network scanners, along with standard operating system commands, can help identify an organization's network security profile and determine whether dangerous services are active in components.
- Modem locators ("war dialing" software) can help identify unsecured dial-in modems.

CAATs can also be used in testing the effectiveness of controls, as a companion to other controls testing. This would typically involve making a small selection of transactions and walking them through the system, or developing an integrated test facility and processing test transactions through the system. The advantage of using CAATs in controls testing is that it is possible to test every transaction (either in a master file or transaction file), to determine whether there were any control failures.

Any analysis performed using CAATS should be adequately documented. In addition, a technical review should be performed by audit staff independent of the preparer to determine that the implementation of CAATS and the analysis of results is complete and accurate and that any conclusions are supported by the analysis.

2.5.3 Use of Sampling Techniques

Controls that leave documented evidence of their existence and application (such as logs) may be tested by inspecting such evidence. If sufficient evidence cannot be obtained through walkthroughs in combination with observation, inquiry, and other tests, the auditor generally should obtain more evidence by using sampling procedures to select individual items for inspection. The auditor may use multipurpose testing to use the same sample to test controls, compliance, and/or substantive results (such as balances in financial statements). Multipurpose testing is usually more efficient than separately designed samples. Alternatively, the auditor may design a sample to test controls alone. In this case, the auditor generally should use random attribute sampling. FAM section 450 (Sampling Control Tests) provides additional information on the use of this sampling technique, including those that can be applied to performance audits.

Exposure Draft

Chapter 3. Evaluating and Testing General Controls

3.0 Introduction

General controls are the policies and procedures that apply to all or a large segment of an agency's information systems and help ensure their proper operation. Examples of primary objectives for general controls are to safeguard data, protect application programs, and ensure continued computer operations in case of unexpected interruptions. General controls are applied at the entitywide, system, and business process application levels. The effectiveness of general controls at the entitywide and system levels is a significant factor in determining the effectiveness of business process controls at the application level. Without effective general controls at the agency and system levels, business process controls generally can be rendered ineffective by circumvention or modification. For example, edits⁴¹ designed to preclude users from entering unreasonably large dollar amounts in a payment processing system can be an effective application control. However, this control cannot be relied on if the general controls permit unauthorized program modifications that might allow some payments to be exempt from the edit. Consequently, the auditor may decide that it is efficient to evaluate the effectiveness of general controls separately from and before evaluating business process controls.

In planning the evaluation of IS controls, the auditor identifies areas of audit interest and critical control points. In identifying these areas, the auditor considers business process applications that are relevant to the audit objectives. Also, the auditor considers the network components that are most significant to the effectiveness of IS controls over the areas of audit interest. In planning the

⁴¹Editing in this context is inspecting a data field or element to verify the accuracy of its content.

Exposure Draft

evaluation of general controls, the auditor considers the most effective and efficient manner to gather evidence to determine the effectiveness of general controls over these critical control points. For example, if a business process application for benefit payments is a key area of audit interest, the auditor's testing of general controls is designed, to the extent possible, to focus on those general controls that most directly affect the application.

The evaluation of general controls includes the following five general control areas:

- security management, which provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the agency's computer-related controls;
- access controls, which limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss, and disclosure;
- configuration management, which prevents unauthorized changes to information system resources (for example, software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended;
- segregation of duties, which includes policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations; and
- contingency planning, so that when unexpected events occur, critical operations continue without disruption or are promptly resumed, and critical and sensitive data are protected.

For each of these five general control areas, this manual identifies several critical elements that are essential for establishing adequate controls. For each critical element, the FISCAM provides a description of risks, control activities, and suggested audit procedures. The auditor can use this information to evaluate agency practices. For each critical element, the auditor should make a summary determination as to the effectiveness of the agency's related controls at the entitywide, system, and application levels. If a

Exposure Draft

critical element is not achieved, the respective control category is not likely to be achieved. The auditor should use professional judgment in making such determinations.

To evaluate the effectiveness of general controls, the auditor identifies control techniques implemented by the agency to address each of the general controls and determine whether these control techniques, as designed, are sufficient to achieve the control. If sufficient, the auditor determines whether they are implemented (placed in operation) and operating effectively. As discussed later in this section, if the control techniques are not sufficient or are not implemented as designed, the auditor should determine the effect on IS controls and the audit objectives.

As discussed in more detail in Chapter 2, general controls are applicable at the entitywide, system, and application levels, and so the auditor should consider general controls at each of these levels. The control techniques and the related audit tests vary according to the level to which they are being applied. However, in this manual they are described at a high level in order to be applicable to many computer environments; they may require some technical expertise about the subject to be effectively performed at an agency. More detailed audit steps generally should be developed by the auditor based on the specific software and control techniques employed by the agency. Table 2 shows the relationship between the general control areas and the levels.

Exposure Draft

Table 2. General Control Categories Applicable at Different Levels of Audit

	Control Categories	Entitywide/ Component Level	System Level			Business Process Application Level
			Network	Operating Systems	Infrastructure Applications	
General Controls	Security Management	→				
	Access Controls	→				
	Configuration Management	→				
	Segregation of Duties	→				
	Contingency Planning	→				

Source: GAO.

The auditor’s evaluation of the effectiveness of IS controls should include system level controls related to each critical control point. Assessing the effectiveness of controls over critical control points should include consideration of all potential ways in which the critical control point could be accessed. Generally, for each critical control point, this would include assessing controls related to the network, operating system, and infrastructure application components. For example, if a particular router was deemed to be a critical control point, the auditor would test controls related to the router itself (a network component), as well as its operating system, and the infrastructure applications used to manage the router. Access to any of these could lead to access to the control point.

To facilitate the auditor’s evaluation, tables identifying commonly used control techniques and related audit procedures are included after the discussion of each critical element and also in Appendix II.

Exposure Draft

These tables can be used for both the preliminary evaluation and the more detailed evaluation and testing of controls. For the preliminary evaluation, the auditor can use the tables to guide and document initial inquiries and observations; for the more detailed evaluation and testing, the auditor can use the suggested procedures in developing and carrying out a testing plan. Such a plan would include more extensive inquiries; inspections of facilities, systems, and written procedures; and tests of key control techniques, which may include using audit or system software and vulnerability analysis tools. To help document these evaluations and allow steps to be tailored to individual audits, electronic versions of the tables are available on our Web site at <http://www.gao.gov/aac.html>.

When evaluating general controls, auditors may want to supplement the control techniques and audit procedures contained in this document with other guidance, including

- National Institute of Standards and Technology (NIST) information security standards and guidelines;
- international security standards published by the International Organization for Standardization and the International Electrotechnical Commission;
- Information Systems Audit and Control Association (ISACA) auditing standards, guidelines, and procedures; and
- requirements unique to the environment and agency being audited.

3.1. Security Management (SM)

An entitywide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Overall policies and plans are developed at the entitywide level. System and application-specific procedures and controls implement the entitywide policy. Without a well-designed program, security controls may be inadequate;

Exposure Draft

responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources. Through FISMA, Congress requires each federal agency to establish an agencywide information security program to provide security to the information and information systems that support the operations and assets of the agency, including those managed by a contractor or other agency.

Security Program Guidance

General guidance on planning and managing an agency information security program is contained in (1) NIST SP 800-12,⁴² which provides guidance on security-related management, operational, and technical controls and (2) our executive guide describing risk management principles found at leading organizations (discussed in the next section).⁴³ In response to FISMA, NIST has since published a series of information security standards and guidelines for agencies to effectively manage risk to agency operations and agency assets. Key publications are:

- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.

FIPS Publication 200 provides

1. a specification for minimum security requirements for federal information and information systems;

⁴²NIST, *An Introduction to Computer Security: The NIST Handbook*, Special Publication (SP) 800-12, October 1995.

⁴³GAO, *Executive Guide: Information Security Management, Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

Exposure Draft

2. a standardized approach to security control selection using the security categorization standard, FIPS Publication 199; and
3. links to NIST SP 800-53, containing the security controls needed for compliance with these minimum security requirements.

In applying the provisions of FIPS 200, agencies first categorize their systems as required by FIPS 199 (see Table 5), and then typically select an appropriate set of security controls from NIST SP 800-53 to satisfy their minimum security requirements. NIST reviews and updates the controls in NIST SP 800-53 annually to ensure that the controls represent the current state of practice in safeguards and countermeasures for information systems.

FIPS 200 and its supporting publication NIST SP 800-53 establish conditions to enable organizations to be flexible in tailoring their security control baselines. Agencies, may, for example, apply scoping guidance taking into consideration the issues related to such things as the technologies employed by the agency, size and complexity of the systems, unique circumstances, and risks involved. Agencies may use compensating controls in lieu of those controls prescribed by NIST SP 800-53. Agencies may also supplement the controls in NIST SP 800-53 with additional controls that may be needed.

In addition, NIST SP 800-100 provides a broad overview of information security program elements, including capital planning and investment control, performance measures, and security services, to assist managers in understanding how to establish and implement an information security program. This handbook summarizes and augments a number of existing NIST standards and guidance documents and provides additional information on related topics.

Other guidance supporting implementation of FIPS 199 and FIPS 200 include:

- NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*

Exposure Draft

- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
- NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*

These and other publications, directives, and policies that support compliance with FISMA are available from NIST's website (<http://csrc.nist.gov>).

Security Management Critical Elements

Assessing an entitywide security management program involves evaluating the agency's efforts to perform each of the critical elements shown in table 3.

Table 3. Critical Elements for Security Management

Number	Description
SM-1	Establish a security management program
SM-2	Periodically assess and validate risks
SM-3	Document security control policies and procedures
SM-4	Implement effective security awareness and other security-related personnel policies
SM-5	Monitor the effectiveness of the security program
SM-6	Effectively remediate information security weaknesses
SM-7	Ensure that activities performed by external third parties are adequately secure

Source: GAO.

The following sections discuss each of these critical elements and the control activities that support their achievement. At the end of each critical element, a summary table is presented that associates each activity with techniques that agencies can use to perform the activity, as well as procedures for auditing the critical elements and control activities.

Critical Element SM-1: Establish a Security Management Program

Agencies should have policies, plans, and procedures that clearly describe the agency's security management program. FISMA

Exposure Draft

requires federal agencies to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The security management program should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security and those who own, use, or rely on the agency's computer resources. As part of this entitywide program, the entity should have a security management structure in place at the system and application levels. Thus, in managing a particular operating system or network device, the agency should have a clearly assigned structure and responsibilities for the security of the operating system and device. Similarly, the entity should have a clearly assigned structure and responsibilities related to particular business process applications. The security program policies, plans, and procedures should be kept up-to-date and revised to reflect system and organizational changes, problems identified during plan implementation, and security control assessments or audit reports.

SM-1.1. The security management program is adequately documented, approved, and up-to-date

The entity's security management program should be adequately documented. The nature and extent of the documentation of the program may vary. For federal entities, at a minimum, the program should adequately reflect the agency's consideration of the following eight elements of an agency wide information security program required by FISMA.

1. periodic risk assessments;
2. policies and procedures to ensure cost-effective risk reduction and compliance with applicable standards and guidance and with agency-determined system configuration requirements;
3. subordinate information security plans for networks, facilities, and systems;
4. security awareness training for agency employees and contractors;

Exposure Draft

5. periodic management testing and evaluation that includes testing of all major systems;
6. a remedial action process to address any deficiencies;
7. security-incident procedures for detecting, reporting, and responding to incidents; and
8. continuity of operations plans and procedures for information systems.

While most of these elements are covered in this section, security incident procedures are covered in section 3.2 on access controls, and continuity of operations is covered in section 3.5 on contingency planning.

The security management program may be documented in the form of a separate written security management program plan or may consist of several documents that collectively record the security management program. The documentation should be supported by subordinate (system and application level) plans and procedures; related policies should cover all major systems and facilities and outline the duties of those responsible for overseeing security (the security management function), as well as those who own, use, or rely on the agency's computer resources. An entitywide plan may describe such things as the overall security architecture, applicable procedures, and applicable system and application-level plans. The system-level plans identify the system-level architecture (for example, network configuration, control points, etc.), operational policies and procedures, and any business process (application-level) plans. Similarly, application-level plans should contain structures, procedures, and controls specific to the application.

The security management program should be approved by an appropriate level of management. In some instances, the entity may include the documentation in a policy document issued by management. In addition, for federal agencies, FISMA requires that the Director of OMB review federal agency security management programs at least annually and approve or disapprove them.

Exposure Draft

Finally, to be effective, the security program documentation should be maintained to reflect current conditions. It should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk due to factors such as changes in entity mission or the types and configuration of computer resources in use. Revisions to policies and plans should be reviewed, approved, and communicated to all employees. Outdated policies and plans not only reflect a lack of adequate top management concern, but also may be ineffective because they may not address current risks.

SM-1.2. A security management structure has been established

Senior management should establish a structure to implement the security management program throughout the entity. The structure generally consists of a core of personnel who are designated as security managers. These personnel play a key role in developing, communicating, and monitoring compliance with security policies and reporting on these activities to senior management. The security management function also serves as a focal point for other personnel who play a role in evaluating the appropriateness and effectiveness of computer-related controls on a day-to-day basis. These personnel include program managers who rely on the agency's computer systems, system administrators, and system users.

As an illustration of the different responsibilities of a security management structure, FISMA establishes responsibilities for certain agency officials as follows:

- The agency head is responsible for (1) providing risk-based information security, (2) complying with FISMA requirements and related NIST standards, (3) ensuring integration of information security management with agency strategic and operational planning, (4) ensuring adequacy of trained information security personnel, and (5) ensuring receipt of annual reporting from the CIO.
- The CIO is to have authority from the agency head to ensure compliance with FISMA, including responsibility for (1) designating a senior agency information security official, (2) developing and maintaining the agency information security program and related policies and procedures, (3) training and

Exposure Draft

overseeing information security personnel, and (4) assisting senior agency officials with their information security responsibilities.

- Senior agency officials are responsible for information security for operations and assets under their control, including (1) assessing risk, (2) determining levels of appropriate security, (3) implementing policies and procedures to cost-effectively reduce risks to an acceptable level, and (4) periodically testing and evaluating security controls.

Our survey of leading organizations⁴⁴ found that a central management focal point is key to ensuring that the various activities associated with managing risk are carried out. Such responsibility is assigned to a central security program office. A central security program office may be supplemented by individual security program managers, designated in units within the entity who assist in the implementation and management of the organization's security program. These individual unit security managers should report to or coordinate with the central security program office.

Responsibilities of the central security program office may include

- facilitating risk assessments,
- coordinating development and distribution of security policies and procedures,
- routinely monitoring compliance with these policies,
- promoting security awareness among system users,
- planning and coordinating security-related activities, including coordination of geographically dispersed security groups,
- ensuring that desktop security plans are integrated with infrastructure and database security plans,

⁴⁴*Executive Guide: Information Security Management, Learning from Leading Organizations* (GAO/AIMD-98-68, May 1998).

Exposure Draft

- providing reports to senior management on policy and control evaluation results and advice to senior management on security policy issues, and
- representing the entity in the security community.

In assessing the effectiveness of the security management structure for an entitywide, system, or application level, the auditor considers the security function's scope of authority, placement, training and experience, and tools. For example, security management personnel should

- have sufficient authority to obtain data needed to monitor compliance with policies, report results to senior management, and elevate concerns regarding inappropriate risk management decisions or practices;
- have sufficient resources to carry out their responsibilities, including staff and tools (for example, computers, established audit trails, and specialized security software);
- report to a level of management that maximizes the independence and objectivity of the security function;
- not be assigned responsibilities that diminish their objectivity and independence; and
- have sufficient training and knowledge of control concepts, computer hardware, software, telecommunications concepts, physical and logical security, data architecture, database management and data access methods, pertinent legislation, and administration and organizational issues.

SM-1.3. Information security responsibilities are clearly assigned

Security-related responsibilities of offices and individuals throughout the entity that should be clearly defined include those of (1) information resource owners and users, (2) information resources management and data processing personnel, (3) senior management, and (4) security administrators. Further, responsibilities for individual employee accountability regarding the use and disclosure of information resources should be established. Appendix III of OMB Circular A-130 requires that the rules of the system and application "shall clearly delineate responsibilities and expected behavior of all individuals with access ... and shall be

Exposure Draft

clear about the consequences of behavior not consistent with the rules.”

Senior management and information resource management have ultimate responsibility for providing direction and ensuring that information security responsibilities are clearly assigned and carried out as intended. Security plans should clearly establish who “owns” the various computer resources, particularly data files, and what the responsibilities of ownership are. Ownership of computer resources should be assigned to persons responsible for their reliability and integrity. For example, owners of data files and application programs are generally the managers of the programs supported by these applications. These managers are primarily responsible for the proper operation of the program and for accurate reporting of related computer data. Similarly, owners of computer facilities and equipment are generally managers who are responsible for the physical protection of these resources. If a resource has multiple owners, policies should clearly describe whether and how ownership responsibilities are to be shared.

Assignment of ownership responsibilities is important because the managers who own the resources are in the best position to (1) determine the sensitivity of the resources, (2) analyze the duties and responsibilities of users, and (3) determine the specific access needs of these users. Once these factors are determined, the resource owner can identify persons authorized to access the resource and the extent of such access. The owners should communicate these authorizations to the security administrators, who are then responsible for implementing access controls in accordance with the owners’ authorizations. Section 3.2, Access Controls, further discusses access authorization.

If management and ownership responsibilities are not clearly assigned, access authorizations may be left to personnel who are not in the best position to determine users’ access needs. Such personnel are likely to authorize overly broad access in an attempt to ensure that all users can access the resources they need. This defeats the purpose of access controls and, depending on the sensitivity of the resources involved, can unnecessarily provide opportunities for fraud, sabotage, and inappropriate disclosures.

Exposure Draft

SM-1.4. Subordinate security plans are documented, approved, and kept up-to-date

Entities should have written security plans at the system and application levels that cover networks, facilities, and systems or groups of systems, as appropriate. The plans and related policies should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security and those who own, use, or rely on the entity's computer resources. In addition, these system-level plans should provide an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. These plans should be kept up-to-date and revised to reflect system and organizational changes, problems identified during plan implementation, and security control assessments or audit reports. NIST SP 800-18 requires that all security plans should be reviewed and updated, if appropriate, at least annually. Further, NIST SP 800-18 and Appendix III of OMB Circular A-130 provide specific guidance on what should be included in federal agency system security plans.

FISMA states that "each agency shall develop, document, and implement...subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." System-level plans should identify the system-level architecture (for example, network configuration, control points, etc.), operational policies and procedures, and any application-level plans. Application plans should contain similar elements such as procedures and controls specific to the application.

System security plans should be clearly documented and, according to Appendix III of OMB Circular A-130, cover each general support system and each major application. The circular further specifies the topics to include in the plans. Topic names will differ depending on whether the plan is for a general support system or a major application, but the subject matter will be similar. The required topics are shown in table 4.

Exposure Draft

Table 4. Security Controls to Include in System Security Plans

General support system	Major application
rules of the system ^a	application rules ^a
training	specialized training
personnel controls	personnel security
incident-response capability	NA
continuity of support	contingency planning
technical security	technical controls
system interconnection	information sharing
NA	public access controls

Source: Appendix III of OMB Circular A-130.

^aThese include rules delineating responsibilities and expected behaviors of staff.

Note: In this manual, access controls are addressed in section 3.2 and contingency planning in section 3.5.

To help ensure that the system security plan is complete and supported by the agency as a whole, senior management should obtain agreement from all affected parties to establish policies for a security program. Such agreements will also help ensure that policies and procedures for security developed at lower levels within the agency are consistent with overall organizational policies and procedures. In accordance with Appendix III of OMB Circular A-130, final responsibility for authorization of a system to process information should be granted by a management official. Generally, the manager whose program operations and assets are at risk is the most appropriate management official. However, any disagreements between program managers and security specialists as to the adequacy of policies and controls should be resolved by senior management.

Like the overall security policies and plans, the subordinate security policies and plans should be maintained to reflect current conditions. As described in SM-1.1, they should be periodically reviewed and updated to reflect changes in risk and revisions should be reviewed, approved, and communicated to employees. Outdated policies and plans may be ineffective because they may not address current risks.

SM-1.5. An inventory of systems is developed, documented, and kept up-to-date

To implement an effective security program, entities need to maintain a complete, accurate, and up-to-date inventory of their

Exposure Draft

systems. Without one, the entity cannot effectively manage IS controls across the entity. For example, effective configuration management requires the entity to know what systems they have and whether the systems are configured as intended. Furthermore, the inventory is necessary for effective monitoring, testing, and evaluation of IS controls, and to support information technology planning, budgeting, acquisition, and management.

FISMA requires that each agency develop, maintain, and annually update an inventory of major information systems operated by the agency or under its control. OMB Circular A-130 defines a major information system as a system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. The inventory must include identification of the interfaces between the agency systems and all other systems or networks, including interfaces not controlled by the agency. The inventory is needed to effectively track the agency systems for annual testing and evaluation and contingency planning.

Control Techniques and Suggested Audit Procedures for Critical Element SM-1

Table 5 presents control activities for critical element SM-1, techniques that entities may use to perform the activity and procedures for auditing the critical element and control activities.

<u>SM-1 Related NIST SP-800-53 Controls</u>

See the first control for each family (e.g., AC-1, AT-1)
--

PL-2 System Security Plan

PL-3 System Security Plan Update

PL-6 Security-Related Activity Planning

SA-2 Allocation of Resources

Exposure Draft

Table 5. Control Techniques and Suggested Audit Procedures for Critical Element SM-1: Establish a security management program

Control activities	Control techniques	Audit procedures
SM-1.1. The security management program is adequately documented, approved, and up-to-date.	<p>SM-1.1.1. An agency/entitywide security management program has been developed, documented, and implemented that</p> <ul style="list-style-type: none"> • covers all major facilities and operations, • has been approved by senior management and key affected parties, and • covers the key elements of a security management program: <ul style="list-style-type: none"> • periodic risk assessments, • adequate policies and procedures, • appropriate subordinate information security plans, • security awareness training, • management testing and evaluation, • a remedial action process, • security-incident procedures, and • continuity of operations. 	<p>Review documentation supporting the agency/entitywide security management program and discuss with key information security management and staff.</p> <p>Determine whether the program</p> <ul style="list-style-type: none"> • adequately covers the key elements of a security management program • is adequately documented, and • is properly approved. <p>Determine whether all key elements of the program are implemented. Consider audit evidence obtained during the course of the audit.</p>
	<p>SM-1.1.2. The agency/entitywide security management program is updated to reflect current conditions.</p>	<p>Based on a review of security management program documentation and interviews with key information security management and staff, determine whether the entity has adequate policies and procedures to identify significant changes in its IT environment that would necessitate an update to the program, and whether the program is periodically updated to reflect any changes.</p>
SM-1.2. A security management structure has been established.	<p>SM-1.2.1. Senior management establishes a security management structure for the entitywide, system, and applications that has adequate independence, authority, expertise, and resources.</p>	<p>Review security policies and plans, the entity's organization chart, and budget documentation. Interview security management staff. Evaluate the security structure: independence, authority, expertise, and allocation of resources required to adequately protect the information systems.</p>
	<p>SM-1.2.2. An information systems security manager has been appointed at an agency/entity level and at appropriate subordinate (i.e., system and application) levels and given appropriate authority.</p>	<p>Review pertinent organization charts and job descriptions.</p> <p>Interview the overall security manager and subordinate security managers responsible for specific systems and applications.</p>
SM-1.3. Information security responsibilities are clearly assigned.	<p>SM-1.3.1. The security program documentation clearly identifies owners of computer-related resources and those responsible for managing access to computer resources. Security responsibilities and expected behaviors are clearly defined at the entitywide, system, and application levels for (1) information resource owners and users, (2) information technology management and staff, (3) senior management, and (4) security administrators.</p>	<p>Review security program documentation detailing security responsibilities and rules of behavior for security officials, resource owners, and users at the entitywide, system, and application levels.</p>

Exposure Draft

Control activities	Control techniques	Audit procedures
SM-1.4. Subordinate security plans are documented, approved, and kept up-to-date.	SM-1.4.1. System and application security plans have been documented and implemented that <ul style="list-style-type: none"> cover all major facilities and operations, have been approved by key affected parties, cover appropriate topics (for federal agencies, those prescribed by OMB Circular A-130; see table 4). 	Review agency/entity policies and procedures for preparing security plans. Review the system and application security plans encompassing key areas of audit interest and critical control points. Determine whether the plans adequately cover appropriate topics (for federal agencies, those prescribed by OMB Circular A-130) and are properly approved. When conducting the audit, determine whether the plans have been implemented and accurately reflect the conditions noted.
	SM-1.4.2. The subordinate security plans are updated on a regular basis or whenever there are significant changes to the agency/entity policies, organization, IT systems, facilities, applications, weaknesses identified, or other conditions that may affect security.	Review relevant security plans and any related documentation indicating whether they have been reviewed and updated and are current.
SM-1.5. An inventory of systems is developed, documented, and kept up-to-date.	SM-1.5.1. A complete, accurate, and up-to-date inventory exists for all major systems that includes the identification of all system interfaces.	Obtain the agency's/entity's systems inventory. Discuss with agency/entity management (1) the methodology and criteria for including or excluding systems from the inventory and (2) procedures and controls for ensuring the completeness, accuracy, and currency of the inventory. Determine whether systems tested during the audit are included in the inventory. Test the inventory for completeness, accuracy, and currency. The objective of this step in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding management's process and controls for ensuring the accuracy of the inventory.

Source: GAO.

Critical Element SM-2. Periodically assess and validate risks

A comprehensive risk assessment should be the starting point for developing or modifying an entity's security policies and security plans. Such assessments are important because they help make certain that all threats and vulnerabilities are identified and considered, that the greatest risks are addressed, and that appropriate decisions are made regarding which risks to accept and which to mitigate through security controls. Appropriate risk assessment policies and procedures should be documented and based on the security categorizations.

Exposure Draft

FISMA, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act, explicitly emphasize a risk-based policy for cost-effective security. In support of and reinforcing this legislation, OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires executive agencies within the federal government to plan for security; ensure that appropriate officials are assigned security responsibility; review the security controls in their information systems; and authorize system processing prior to operations and periodically thereafter.

Risk assessments should consider threats and vulnerabilities at the entitywide level, system level, and application levels. For example, at the entitywide level, risk assessments should consider personnel policies and procedures, training, and security awareness activities. At the system level, risks related to connectivity issues (for example, Internet, dial-up, wireless) and access controls (for example, both logical and physical) need to be assessed. At the application level, risk assessments need to consider specific business processes and highly-integrated enterprise resource planning (ERP) applications (discussed in Chapter 4).

Risk assessments should consider risks to data confidentiality, integrity, and availability, and the range of risks that an entity's systems and data may be subject to, including those posed by authorized internal and external users, as well as unauthorized outsiders who may try to break into the systems. For example, risk assessments should take into account observed trends in the types and frequency of hacker activity and threats. Such analyses should also draw on reviews of system and network configurations, as well as observations and testing of existing security controls.

Our study of security programs at leading organizations found that the following were key success factors for risk assessments.

- Organizations had a defined process that allowed an entitywide understanding of what a risk assessment was and avoided individual units developing independent definitions.
- Organizations required that risk assessments be performed and designated a central security group to schedule and facilitate them.

Exposure Draft

- Risk assessments involved a mix of individuals who have knowledge of business operations and technical aspects of the organization's systems and security controls.
- The business managers were required to provide a final sign-off indicating agreement with risk-reduction decisions and acceptance of the residual risk.
- Organizations required that final documentation be forwarded to more senior officials and to internal auditors so that participants could be held accountable for their decisions.
- Leading organizations did not attempt to precisely quantify risk. Although they would have liked to place a dollar value on risks and precisely quantify the costs and benefits of controls, they felt that spending time on such an exercise was not worth the trouble. They believed that few reliable data were available on either the actual frequency of security incidents or on the full costs of controls and of damage due to a lack of controls.

Risk assessments are more likely to be effective when performed by personnel with enough independence to be objective and with enough expertise (training and experience) to be able to adequately identify and assess technical and security risks.

Risk assessment and risk management are ongoing efforts. Although a formal, comprehensive risk assessment is performed periodically, such as part of a system security plan, risk should be considered whenever there is a change in an entity's operations or its use of technology or in outside influences affecting its operations. Changes to systems, facilities, or other conditions and identified security vulnerabilities should be analyzed to determine their impact on risk, and the risk assessment should be performed or revised as necessary. The risk assessment and validation and related management approvals should be documented and maintained on file. Such documentation should include risk assessments, security test and evaluation results, security plans, and appropriate management approvals. Further, according to NIST SP 800-37, systems should be certified and accredited before being placed in operation and when major system changes occur.

Exposure Draft

The NIST SP 800-30 risk management guide discusses the development of an effective risk management program and contains both the definitions and the practical steps necessary for assessing and mitigating risks within IT systems. According to this guide, the principal goal of an entity's risk management process should be to protect the entity and its ability to perform its mission, not only its information technology assets.

According to FISMA, federal agencies must periodically assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support their operations and assets. Policies and procedures are based on risk, and the rigor of management testing and evaluation of information security should also be based on risk. Also, the Federal Managers' Financial Integrity Act of 1982 requires agencies to conduct risk assessments to identify and prioritize their vulnerabilities to waste, fraud, and abuse; Appendix III of OMB Circular A-130 requires that agencies consider risk when determining the need for and selecting computer-related control techniques. However, the Circular no longer requires formal periodic risk analyses that attempt to quantify in dollars an annual loss exposure resulting from unfavorable events.

Pursuant to FISMA, NIST developed standards for security categorization of federal information and information systems according to a range of potential impacts (FIPS Pub 199). Table 6 summarizes these NIST standards using potential impact definitions for each security objective (confidentiality, integrity, and availability). Federal agencies should categorize/classify their non-national security systems according to these impact levels. The security categories are based on the potential impact on an agency should certain events occur that jeopardize the information and information systems needed by the agency to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. NIST also issued a guide for mapping types of information and information systems to security categories (NIST SP 800-60). Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an agency.

Exposure Draft

Table 6. NIST Impact Definitions for Security Objectives

Security objective	Potential impact		
	Low	Moderate	High
<p><i>Confidentiality</i> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. {44 U.S.C., Sec 3542}</p>	<p>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<p><i>Integrity</i> Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. {44 U.S.C., Sec 3542}</p>	<p>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>

Exposure Draft

Security objective	Potential impact		
	Low	Moderate	High
<p><i>Availability</i> Ensuring timely and reliable access to and use of information. {44 U.S.C. 3542}</p>	<p>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>

Source: National Institute of Standards and Technology (NIST), FIPS Publication 199, page 6.

One area that merits additional emphasis is the appropriate consideration of risks associated with sensitive privacy information. In addition to an appropriate consideration of related risk, specific controls are discussed at SM-5 and AC-4.2.

In addition to FISMA, federal agencies are subject to privacy laws aimed at preventing the misuse of personally identifiable information.⁴⁵ The Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002 contain the major requirements for the protection of personal privacy by federal agencies. The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records⁴⁶ and requires that when agencies establish or make changes to a system

⁴⁵ Personally identifiable information refers to any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, or biometric records, and any other information which is linked or linkable to an individual.

⁴⁶ The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also identifies "system of records" as a group of records under the control of any agency retrieved by the name of the individual or by an individual identifier.

Exposure Draft

of records; they must notify the public by a “system-of-records notice.”⁴⁷ The E-Government Act of 2002 strives to enhance protection for personal information in government information systems or information collections by requiring that agencies conduct privacy impact assessments. These privacy impact assessments include an analysis of how personal information is collected, stored, shared, and managed in a federal system.

According to OMB guidance, these privacy impact assessments must analyze and describe how the information will be secured including administrative and technological controls and should be current.⁴⁸

As discussed in NIST SP 800-60⁴⁹, in establishing confidentiality impact levels for each information type, responsible parties must consider the consequences of unauthorized disclosure of privacy information (with respect to violations of Federal policy and/or law). The impact of privacy violations will depend in part on the penalties associated with violation of the relevant statutes and policies. Further, it says that, in most cases, the impact on confidentiality for privacy information will be in the *moderate* range.

<u>SM-2 Related NIST SP-800-53 Controls</u>

CA-4 Security Certification

CA-6 Security Accreditation

RA-2 Security Categorization

RA-3 Risk Assessment

RA-4 Risk Assessment Update

⁴⁷ A system of records notice is a notice in the Federal Register identifying, among other things, the type of data collected, the types of individuals about whom information is collected, the intended “routine” uses of data, and procedures that individuals can use to review and correct personal information.

⁴⁸ According to FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, OMB Memorandum M-06-20, July 17, 2006, a privacy impact assessment or a system of records notice is current if that document satisfies the applicable requirements and subsequent substantial changes have not been made to the system.

⁴⁹ NIST Special Publication (SP) 800-60, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories* (June 2004)

Exposure Draft

Control Techniques and Suggested Audit Procedures for Critical Element SM-2

Table 7 Control Techniques and Suggested Audit Procedures for Critical Element SM-2: Periodically assess and validate risks

Control activities	Control techniques	Audit procedures
SM-2.1. Risk assessments and supporting activities are systematically conducted.	SM-2.1.1. Appropriate risk assessment policies and procedures are documented and based on security categorizations.	Review risk assessment policies, procedures, and guidance.
	SM-2.1.2. Information systems are categorized based on the potential impact that the loss of confidentiality, integrity, or availability would have on operations, assets, or individuals.	Determine if security risk categorizations are documented and, for federal entities, if they comply with FISMA, NIST FIPS Pub 199 and SP 800-60.
	SM-2.1.3. Risks are reassessed for the entitywide, system, and application levels on a periodic basis or whenever systems, applications, facilities, or other conditions change.	Obtain the most recent risk assessments encompassing key areas of audit interest and critical control points. Determine if the risk assessments are up-to-date, appropriately documented, approved by management, and supported by sufficient testing. For federal systems, consider compliance with FISMA, OMB, and NIST requirements/guidance and whether the technology used is appropriately considered in the risk assessment and validations. The objective of this step in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding management's risk assessment process (including related controls), reading the risk assessments for the key systems relevant to the audit objectives, and determining whether risks identified by the IS controls audit are properly considered in the risk assessments.
	SM-2.1.4. Risk assessments and validations, and related management approvals are documented and maintained on file. Such documentation includes security plans, risk assessments, security test and evaluation results, and appropriate management approvals.	For a selection of risk assessments determine whether required management approvals are documented and maintained on file.
	SM-2.1.5. Changes to systems, facilities, or other conditions and identified security vulnerabilities are analyzed to determine their impact on risk and the risk assessment is performed or revised as necessary based on OMB criteria.	Review criteria used for revising risk assessments. For recent changes that meet the criteria, determine if the risk assessment was redone or updated.

Exposure Draft

SM-2.1.6. Federal systems are certified and accredited before being placed in operation and at least every 3 years, or more frequently if major system changes occur.

For federal systems that are significant to the audit objectives,, review certification and accreditation documentation and determine compliance with NIST SP 800-37. The objective of this step in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding the certification and accreditation process (including related controls), reading the certifications and accreditations for the key systems relevant to the audit objectives, and determining whether the certification and accreditation documentation for the systems tested is consistent with the testing results.

Source: GAO.

Critical Element SM-3. Document security control policies and procedures

Security control policies and procedures should be documented and approved by management. They should also appropriately consider risk, address general and application controls, and ensure that users can be held accountable for their actions. Control policies and procedures may be written to be more general at the entitywide level and more specific at the systems (for example, specific configurations) and application levels (for example, user access rules for specific applications). For example, access control policies may be implemented at the entitywide level through communication of formal written guidance; at the system level through system-level security software, firewall rules, and access control lists; and at the application level through very specific controls built into the application. Also, a formal sanctions process should be established for personnel who fail to comply with established IS control policies and procedures.

According to FISMA, each agency information security program must include policies and procedures that are based on risk assessments that cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system. NIST provides guidance pertaining to computer security policy and procedures, described here.

Exposure Draft

Security policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. The term is also used to refer to the specific security rules for particular systems. Because policy is written at a broad level, agencies also develop standards, guidelines, and procedures that offer users, managers, and others a clear approach to implementing policy and meeting organizational goals. Standards and guidelines specify technologies and methodologies to be used to secure systems. Standards, guidelines, and procedures may be promulgated throughout an entity via handbooks, regulations, or manuals.

Procedures are detailed steps to be followed to accomplish particular security-related tasks (for example, preparing new user accounts and assigning the appropriate privileges). Procedures provide more detail in how to implement the security policies, standards, and guidelines. Manuals, regulations, handbooks, or similar documents may mix policy, guidelines, standards, and procedures, since they are closely linked. In order for manuals and regulations to serve as important tools, they should clearly distinguish between policy and its implementation. This can help in promoting flexibility and cost-effectiveness by offering alternative approaches to implementing policies.

<u>SM-3 Related NIST SP-800-53 Controls</u>

See the first control for each family (e.g., AC-1, AT-1)
--

Exposure Draft

Control Techniques and Suggested Audit Procedures for Critical Element SM-3

Table 8. Control Techniques and Suggested Audit Procedures for Critical Element SM-3: Document security control policies and procedures

Control activities	Control techniques	Audit procedures
SM-3.1 Security control policies and procedures are documented, approved by management and implemented.	SM-3.1.1. Security control policies and procedures at all levels <ul style="list-style-type: none">• are documented,• appropriately consider risk,• address purpose, scope, roles, responsibilities, and compliance,• ensure that users can be held accountable for their actions,• appropriately consider general and application controls,• are approved by management, and• are periodically reviewed and updated.	Review security policies and procedures at the entitywide level, system level and application level. Compare the content of the policies and procedures to NIST guidance (e.g. SP 800-30, SP 800-37, SP 800-100) and other applicable criteria (e.g. configuration standards).

Source: GAO.

Critical Element SM-4. Implement effective security awareness and other security-related personnel policies

Effective security-related personnel policies are critical to effective security. Ineffective personnel policies can result in employees or contractors inadvertently or intentionally compromising security. For example, security may be compromised due to an inadequate awareness or understanding, inadequate security training, or inadequate screening of employees.

An ongoing security awareness program should be implemented that includes first-time training for all new employees, contractors, and users; periodic refresher training for all employees, contractors and users; and distribution of security policies detailing rules and expected behaviors to all affected personnel. Relevant security awareness requirements and guidance are contained in FISMA, OMB Circular A-130, and NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*. In addition, employees with significant security responsibilities should receive specialized training, as described in NIST SP 800-16, *“Information Technology Security Training Requirements: A Role- and Performance-Based Model”* (April 1998).

Exposure Draft

According to FISMA, an agencywide information security program must include security awareness training for not only agency personnel but also contractors and other users of information systems that support the agency's operations and assets. This training must cover (1) information security risks associated with users' activities and (2) users' responsibilities in complying with agency policies and procedures designed to reduce these risks. FISMA also includes requirements for training of personnel with significant responsibilities for information security. Further, OMB requires personnel to be trained before they are granted access to systems or applications. The training is to make sure that personnel are aware of the system or application's rules, their responsibilities, and their expected behavior.

Other security-related personnel policies are also relevant to effective security. Policies related to personnel actions, such as hiring, termination, and employee expertise, are important considerations in securing information systems. If personnel policies are not adequate, an entity runs the risk of (1) hiring unqualified or untrustworthy individuals; (2) providing terminated employees opportunities to sabotage or otherwise impair entity operations or assets; (3) failing to detect continuing unauthorized employee actions; (4) lowering employee morale, which may in turn diminish employee compliance with controls; and (5) allowing staff expertise to decline.

As mentioned, FISMA requires agencies to implement agencywide security programs that include effective policies and procedures to ensure cost-effective risk reduction and ensure compliance with FISMA and applicable OMB (e.g., OMB Circular A-130) and NIST (e.g., SP 800-30) guidance. This guidance specifically addresses security-related personnel policies and procedures. For example, NIST SP 800-53 addresses personnel security and controls related to personnel screening, termination and transfer, and third-party security.

Exposure Draft

SM-4.1 Ensure that resource owners, system administrators, and users are aware of security policies

For a security program to be effective, those expected to comply with it must be aware of it. Typical means for establishing and maintaining security awareness include

- informing users of the importance of the information they handle and the legal and business reasons for maintaining its integrity and confidentiality;
- distributing documentation describing security policies, procedures, and users' responsibilities, including their expected behavior;
- requiring users to periodically sign a statement acknowledging their awareness and acceptance of responsibility for security (including the consequences of security violations) and their responsibilities for following all organizational policies (including maintaining confidentiality of passwords and physical security over their assigned areas); and
- requiring comprehensive security orientation, training, and periodic refresher programs to communicate security guidelines to both new and existing employees and contractors.

The leading organizations studied considered promoting awareness to be one of the most important factors in the risk management process. Awareness was considered to be especially important in reducing the risks of "social engineering," where users are talked into revealing passwords or other sensitive information to potential thieves. Educating users about such risks makes them think twice before revealing sensitive data and makes them more likely to notice and report suspicious activity.

Employee awareness is also critical in combating security threats posed by spam, spyware, and phishing. Spam (unsolicited commercial e-mail) consumes significant resources and is used as a delivery mechanism for other types of cyberattacks; spyware (software that monitors user activity without user knowledge or consent) can capture and release sensitive data, make unauthorized changes, and decrease system performance; and phishing (fraudulent messages to obtain personal or sensitive data) can lead to identity theft, loss of sensitive information, and reduced trust and

Exposure Draft

use of electronic government services. The blending of these threats creates additional risks that cannot be easily mitigated with currently available tools.

SM-4.2. Hiring, transfer, termination, and performance policies address security

The security policies and procedures (including relevant personnel and human resources policies and procedures) that should generally be in place include the following:

- Hiring procedures include contacting references, performing background investigations, and ensuring that periodic investigations are performed as required by law and implementing regulations, consistent with the sensitivity of the position, per criteria from the Office of Personnel Management.
- Individuals are screened before they are authorized to have access to organizational information and information systems.
- For employees and contractors assigned to work with confidential information, confidentiality, nondisclosure, or security access agreements specify precautions required and unauthorized disclosure acts, contractual rights, and obligations during employment and after termination.
- Periodic job rotations and vacations are used, if appropriate, and work is temporarily reassigned during vacations.
- A formal sanctions process enforces (including performance ratings for individual employees) compliance with security policies and procedures.
- Compensation and recognition are appropriate to promote high morale.
- Where appropriate, termination and transfer procedures include
 - exit interview procedures;
 - return of property, such as keys, identification cards, badges, and passes;
 - notification to security management of terminations, and prompt termination of access to the agency's resources and facilities (including passwords);

Exposure Draft

- the immediate escorting of terminated employees—especially those who have access to sensitive resources—out of the agency’s facilities; and
- identification of the period during which nondisclosure requirements remain in effect.

SM-4.3. Employees have adequate training and expertise

Management should ensure that employees—including data owners, system users, data processing personnel, and security management personnel—have the expertise to carry out their information security responsibilities. To accomplish this, a security training program should be developed that includes

- job descriptions that include the education, experience, and expertise required;
- periodically reassessing the adequacy of employees’ skills;
- annual training requirements and professional development programs to help make certain that employees’ skills, especially technical skills, are adequate and current; and
- monitoring employee training and professional development accomplishments.

SM-4 Related NIST SP-800-53 Controls

AT-2 Security Awareness
AT-3 Security Training
AT-4 Security Training Records
PL-4 Rules of Behavior
PS-1 Personnel Security Policy and Procedures
PS-2 Position Categorization
PS-3 Personnel Screening
PS-4 Personnel Termination
PS-5 Personnel Transfer
PS-6 Access Agreements
PS-7 Third-Party Personnel Security
PS-8 Personnel Sanctions

Exposure Draft

Control Techniques and Suggested Audit Procedures for Critical Element SM-4

Table 9. Control Techniques and Suggested Audit Procedures for Critical Element SM-4: Implement effective security awareness and other security-related personnel policies

Control activities	Control techniques	Audit procedures
SM-4.1. Owners, system administrators, and users are aware of security policies.	SM-4.1.1. An ongoing security awareness program has been implemented that includes security briefings and training that is monitored for all employees with system access and security responsibilities. Coordinate with the assessment of the training program in SM-4.3.	Review documentation supporting or evaluating the awareness program. Observe a security briefing. Interview data owners, system administrators, and system users. Determine what training they have received and if they are aware of their security-related responsibilities.
	SM-4.1.2. Security policies are distributed to all affected personnel, including system and application rules and expected user behaviors.	Review memos, electronic mail files, or other policy distribution mechanisms. Review personnel files to test whether security awareness statements are current. If appropriate, call selected users, identify yourself as security or network staff, and attempt to talk them into revealing their password.
SM-4.2. Hiring, transfer, termination, and performance policies address security.	SM-4.2.1. For prospective employees, references are contacted and background checks performed. Individuals are screened before they are given authorization to access organizational information and information systems.	Review hiring policies. For a selection of recent hires, inspect personnel records and determine whether references have been contacted and background checks have been performed.
	SM-4.2.2. Periodic reinvestigations are performed as required by law, and implementing regulations [at least once every 5 years], consistent with the sensitivity of the position per criteria from the Office of Personnel Management (OPM).	Review applicable laws, regulations and reinvestigation policies (e.g. 5CFR 731.106(a); OPM/Agency policy, regulations and guidance; FIPS 201 & NIST SP 800-73, 800-76, 800-78; and, any criteria established for the risk designation of the assigned position.) For a selection of sensitive positions, inspect personnel records and determine whether background reinvestigations have been performed as required.
	SM-4.2.3. Nondisclosure or security access agreements are required for employees and contractors assigned to work with confidential information.	Review policies on confidentiality or security agreements. For a selection of such users, determine whether confidentiality or security agreements are on file.
	SM-4.2.4. When appropriate, regularly scheduled vacations exceeding several days are required, and the individual's work is temporarily reassigned.	Review vacation policies. Inspect personnel records to identify individuals who have not taken vacation or sick leave in the past year. Determine who performed employee's work during vacations.

Exposure Draft

Control activities	Control techniques	Audit procedures
	SM-4.2.5. A formal sanctions process is employed for personnel failing to comply with security policy and procedures.	Review the sanctions process. Determine how compliance with security policies is monitored and how sanctions were administered.
	SM-4.2.6. Where appropriate, termination and transfer procedures include <ul style="list-style-type: none"> • exit interview procedures; • return of property, keys, identification cards, passes, etc.; • notification to security management of terminations and prompt revocation of IDs and passwords; • immediate escort of terminated employees out of the agency's facilities; and • identification of the period during which nondisclosure requirements remain in effect. 	Review pertinent policies and procedures. For a selection of terminated or transferred employees, examine documentation showing compliance with policies. Compare a system-generated list of users to a list of active employees obtained from personnel to determine whether IDs and passwords for terminated employees still exist.
SM-4.3. Employees have adequate training and expertise.	SM-4.3.1. Skill needs are accurately identified and included in job descriptions, and employees meet these requirements.	Review job descriptions for security management personnel and for a selection of other personnel. For a selection of employees, compare personnel records on education and experience with job descriptions.
	SM-4.3.2. A security training program has been developed and includes first-time security awareness training entitywide for all new employees, contractors, and users before they are authorized to access the system, and periodic refresher training thereafter; technical training for personnel with significant system roles and responsibilities before they are authorized access to the system; and periodic refresher training thereafter; and documented entitywide security training records that are monitored for all employees who have system access and security responsibilities.	Review training program documentation. See NIST SP 800-16 and 800-50 for guidance. Coordinate with the assessment of security awareness in SM-4.1.
	SM-4.3.3. Employee training and professional development are documented and monitored.	Review training records and related documentation showing whether such records are monitored and whether employees are receiving the appropriate training.

Source: GAO.

Critical Element SM-5. Monitor the effectiveness of the security program

An important element of risk management is ensuring that policies and controls intended to reduce risk are effective on an ongoing basis. Effective monitoring involves the entity performing tests of IS controls to evaluate or determine whether they are appropriately designed and operating effectively to achieve the entity's control objectives. Senior management's awareness, support, and involvement are essential in establishing the control environment needed to promote compliance with the agency's/entity's

Exposure Draft

information security program. However, because security is not an end in itself, senior managers should balance the emphasis on security with the larger objective of achieving the agency's/entity's mission. To do this effectively, top management should understand the agency's/entity's security risks and actively support and monitor the effectiveness of its security policies. If senior management does not monitor the security program, it is unlikely that others in the organization will be committed to properly implementing it. Monitoring is one of GAO's five internal control standards.⁵⁰

Over time, policies and procedures may become inadequate because of changes in threats, changes in operations or deterioration in the degree of compliance. Periodic assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan. Such assessments can be performed by entity staff or by external reviewers engaged by management. Independent audits performed or arranged by GAO and by agency inspectors general, while an important check on management performance, should not be viewed as substitutes for management evaluations of the adequacy of the agency's security program.

FISMA requires periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices. First, agencies must provide management testing of every system every year, but the level of rigor may vary depending on the risk. However, OMB in past FISMA reporting guidance (M-03-19) has noted that annual FISMA testing does not alter OMB's policy requiring system reauthorization (certification and accreditation) at least every 3 years or when significant changes are made.⁵¹ Second, FISMA requires annual independent evaluations of agency information security programs and practices to determine their effectiveness. These independent evaluations must test the

⁵⁰ Standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1; November 1999).

⁵¹ OMB's Circular A-130 requires that agencies review security controls and re-authorize system usage (i.e., certification and accreditation) at least every three years or more frequently if changes occur.

Exposure Draft

effectiveness of control techniques for a representative subset of systems.

As part of its monitoring function, management should have policies and procedures for periodically assessing the appropriateness of security policies and the agency's compliance with them. At a minimum, such policies and procedures should address the following areas:

- **Frequency of periodic testing.** The frequency, nature, and extent of management's assessment should appropriately consider information security risks. Consequently, certain higher-risk systems may be tested more frequently or more extensively than lower-risk systems. FISMA requires periodic testing to be performed with a frequency depending on risk, but no less than annually.
- **Depth and breadth of testing.** The depth and breadth of testing should be based on a consideration of potential risk and magnitude of harm, the relative comprehensiveness of prior reviews, the nature and extent of tests performed as part of periodic risk and vulnerability assessments, and the adequacy and successful implementation of remediation plans.
- **Common controls.** To facilitate efficient periodic testing, entities should identify common IS controls that can be tested and the results used for multiple systems.
- **Roles and responsibilities of personnel involved in testing.** Personnel assigned to perform and supervise periodic testing should possess appropriate technical skills and have appropriate organizational placement to reasonably assure that tests are properly performed and results properly reported to entity management. In addition, personnel should not perform tests of controls for which they are responsible for implementation or operation.
- **Documentation.** Tests performed and the results and related analysis of such tests should be documented to the extent

Exposure Draft

necessary to support effective supervisory review and independent evaluation.

An integrated testing plan or strategy helps to facilitate effective and efficient periodic testing. Without such an integrated plan or strategy, the nature and extent of periodic testing may be inadequate or testing may be inefficient.

Such tests may include tests performed as part of periodic risk and vulnerability assessments, continuous monitoring through scanning or agent-based software tools, or specifically designed tests. Management should periodically perform vulnerability assessments to help ensure that entity information resources are adequately protected. Vulnerability assessments involve analyzing a network to identify potential vulnerabilities that would allow unauthorized access to network resources, simulating what might be performed by someone trying to obtain unauthorized access. Vulnerability assessments typically consider both unauthorized access by outsiders as well as insiders. Vulnerability assessments typically include the use of various tools discussed in Table 10 below, such as scanning tools, password crackers, and war dialing and war driving tools. Also, vulnerability assessments may include penetration testing. Vulnerability assessments should be performed in addition to testing individual access controls and other control categories.

Since the methods used for unauthorized access vary greatly and are becoming more sophisticated, the vulnerability assessment techniques defined here are general in nature and should be supplemented with techniques and tools specific to the specific environment.

The effectiveness of management's security testing, including vulnerability assessments, may affect the auditor's judgements about audit risk and consequently, the nature, timing, and extent of audit testing. Factors to consider in assessing the effectiveness of management's testing include:

- the nature of management's testing (the types of testing management applied, the strength of the evidence obtained, the experience, capabilities, and objectivity of the persons

Exposure Draft

performing the testing, and the quality of documentation of testing),

- the timing of management’s testing (the recentness of testing), and
- extent of management’s testing (the completeness of testing)

The auditor should review management vulnerability assessments and may independently perform their own vulnerability assessments to determine whether management vulnerability assessments are effective.

The type of vulnerability assessments that are conducted by the auditor affect the scope of the evaluation, methodology used, and the level of assurance achieved. It is important that the methods chosen by the auditor provide the least amount of disruption to the entity based on a cost/risk analysis. Auditors may need to conduct these types of audits without tools,⁵² because some audited entities will not want to accept the risk of an auditor running tools in a “live” environment. There should be an agreement between the auditor and the audited entity on the type of testing to be conducted (intrusive or nonintrusive). Section 2.1.9.E “Communication with Entity Management and Those Charged With Governance” provides further guidance on communicating the nature and extent of planned testing with the entity.

Due to the highly technical nature of such testing by the auditor, it should be performed by persons possessing the necessary technical skills (e.g., an IT specialist). See Appendix V for additional information on the Knowledge, Skills, and Abilities needed to perform IS control audits. Also, section 2.5.2 “Automated Audit Tools” provides further guidance on the auditor’s use of testing tools. Audit testing is discussed further in connection with AC-1.1.

⁵²Assessments performed relying on reviews of system documentation such as hardware and software security settings and use of software features that are inherent to the application under review.

Exposure Draft

There are several different types of security testing. Some testing techniques are predominantly manual, requiring an individual to initiate and conduct the test. Other tests are highly automated and require less human involvement. Testing may also be conducted from external connections (for example, from the Internet, dial-up, wireless), from wide area network connections, or from internal connections. Regardless of the type of testing, staff that set up and conduct security testing should have significant security and networking knowledge, including significant expertise in the following areas: network security, firewalls, intrusion detection systems, operating systems, programming and networking protocols (such as Transmission Control Protocol/Internet Protocol (TCP/IP) – which is a low-level communication protocol that allows computers to send and receive data).

Table 10 summarizes types of security testing.

Table 10. Types of Security Testing

Test type	What it does
Network scanning	<ul style="list-style-type: none">• Enumerates the network structure and determines the set of active hosts and associated software• Identifies unauthorized hosts connected to a network• Identifies open ports• Identifies unauthorized services
General vulnerability scanning	<ul style="list-style-type: none">• Enumerates the network structure and determines the set of active hosts and associated software• Identifies a target set of computers to focus vulnerability analysis• Identifies potential vulnerabilities on the target set• Verifies that software (e.g., operating systems and major applications) is up-to-date with security patches and software versions
Penetration testing	<ul style="list-style-type: none">• Determines how vulnerable an organization's network is to penetration and the level of damage that can be incurred• Tests IT staff's response to perceived security incidents and their knowledge of and implementation of the organization's security policy and system's security requirements• Verifies potential impact of multiple security weaknesses
Password cracking	<ul style="list-style-type: none">• Verifies that the policy is effective in producing passwords that are more or less difficult to break• Verifies that users select passwords that are compliant with the organization's security policy
Log reviews	<ul style="list-style-type: none">• Verifies that the system is operating according to policy
Integrity checkers	<ul style="list-style-type: none">• Detects unauthorized file modifications

Exposure Draft

Test type	What it does
Virus detectors	<ul style="list-style-type: none">• Detects and deletes viruses before successful installation on the system
War dialing	<ul style="list-style-type: none">• Detects unauthorized modems and prevents unauthorized access to a protected network
War driving	<ul style="list-style-type: none">• Detects unauthorized wireless access points and prevents unauthorized access to a protected network
Specialty scanning tools	<ul style="list-style-type: none">• Detects security risks related to specific IS control areas (e.g., weaknesses in web pages, application code, and databases, network sniffers⁵³)

Source: Guideline on Network Security Testing (NIST SP 800-42, October 2003).

Often, several of these testing techniques are used together for a more comprehensive assessment of the overall network security posture. For example, penetration testing usually includes network scanning and vulnerability scanning to identify vulnerable hosts and services that may be targeted for later penetration. Some vulnerability scanners incorporate password cracking. None of these tests by themselves will provide a complete picture of the network or its security posture. NIST SP 800-42 describes these testing types in detail and summarizes the strengths and weaknesses of each test.

However, since penetration testing requires extensive planning and experienced staff to conduct, the auditor typically considers several factors before deciding to perform this testing. For example, penetration testing may be a desirable testing option when significant changes have been made to the entity's network (e.g., upgrades to server, routers, switches, network software), there are no recent penetration tests performed, or results of recent penetration testing identified significant security weaknesses that management represented were substantially corrected. Conversely, if recent penetration testing disclosed few security weaknesses and the scope and level of testing is determined by the auditor to be sufficient, then the use of other types of testing may be more appropriate.

⁵³ Network "sniffers" (software that can intercept and log traffic passing over a network) can identify the transmission of passwords or sensitive information in clear text.

Exposure Draft

Other tools that may be used include specialty scanning tools (for example, application code, Web, database, SNMP⁵⁴), host data extraction tools, packet analyzers or sniffers (for example, ethereal), and patch assessment tools. Separate patch assessment tools are more reliable than vulnerability scanners for this purpose. Also, the auditor is more likely to check for the presence of integrity checkers and virus detectors than to use them in an audit. After running any tests, certain procedures should be followed, including documenting the test results, informing system owners of the results, and ensuring that vulnerabilities are patched or mitigated.

When implementing system security plans for federal systems, as required by FISMA and OMB Circular A-130, management should monitor their implementation and adjust the plans in accordance with changing risk factors. Management should

- develop and document appropriate testing policies and procedures (all levels),
- test and document security controls related to each major system at least annually (system level),
- ensure that the frequency and scope of testing is commensurate with risk (all levels), and
- employ automated mechanisms to verify the correct operation of security functions when anomalies are discovered (system and application level).

In addition to the FISMA provisions in the E-Government Act of 2002, Section 208 requires that agencies conduct privacy impact assessments. A privacy impact assessment is an analysis of how information is handled (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to

⁵⁴SNMP (Simple Network Management Protocol) provides remote administration of network devices.

Exposure Draft

mitigate potential privacy risks (OMB Memorandum M-03-22). OMB combined the FISMA and privacy annual reporting beginning in fiscal year 2005 (OMB Memorandum M-05-15).

Further, OMB has developed performance measures for federal agency reporting and requires that agencies provide quarterly performance metric updates. For example, one such measure requests the number of systems for which security controls have been tested and evaluated in the past year. Incomplete reporting on OMB's performance measures will be noted in OMB's public report to Congress and will be a consideration in OMB's annual approval or disapproval of the agency's security program. NIST SP 800-55 provides additional guidance on performance measures and compliance metrics to monitor the security process and periodically report on the state of compliance.

In addition, NIST SP 800-100 provides information on how entities can develop information security metrics that measure the effectiveness of their security program, and provide data to be analyzed and used by program managers and system owners to isolate problems, justify investment requests, and target funds specifically to the areas in need of improvement. It describes metric types and discusses development and implementation approaches.

As mentioned, OMB Circular A-130 requires that federal agencies review and test the security of their general support systems and major applications at least once every 3 years—sooner if significant modifications have occurred or where the risk and magnitude of harm are high. Although not required, it would be appropriate for an agency to describe its evaluation program, including the expected type of testing and frequency of evaluations, in its security plan. (Security plans are discussed in critical element SM-1.)

OMB also requires that a management official authorize in writing the use of each general support system and major application. NIST SP 800-37 refers to this authorization as accreditation. OMB Circular A-130 allows self-reviews of controls for general support systems, but requires an independent review or audit of major applications. The authorizations or accreditations are to be provided by the program or functional managers whose missions are supported by

Exposure Draft

the automated systems; these represent the managers' explicit acceptance of risk based on the results of any security reviews, including those performed as part of financial statement audits and during related risk assessments. Additional guidance on accrediting federal automated systems can be found in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

In addition, the Federal Managers' Financial Integrity Act of 1982 (FMFIA) and OMB Circular A-123⁵⁵ require agencies to annually assess their internal controls, including computer-related controls, and report any identified material weaknesses to the President and the Congress. The quality of the FMFIA process is a good indicator of management's (1) philosophy and operating style, (2) methods of assigning authority and responsibility, and (3) control methods for monitoring and follow-up. Weaknesses identified during security reviews conducted under OMB Circular A-130 are to be considered for reporting under FMFIA and OMB Circular A-123, particularly if the weakness involves no assignment of security responsibility, an inadequate security plan, or missing management authorization.

FISMA requires that each agency conduct an annual independent evaluation to determine the effectiveness of its information security program and practices. This evaluation must include testing of information security policies, procedures, and practices of a representative subset of the agency's information systems. The head of each agency must report the evaluation results to OMB, which summarizes the results in a report to the Congress. GAO must also provide Congress with its independent assessment of agency information security policies and practices, including compliance with the annual evaluation and reporting requirements.

⁵⁵Office of Management and Budget, *Management's Responsibility for Internal Control*, OMB Circular No. A-123 (Washington, D.C.: December 2004).

Exposure Draft

SM-5 Related NIST SP-800-53 Controls
 CA-2 Security Assessments
 CA-7 Continuous Monitoring
 PL-5 Privacy Impact Assessment
 RA-5 Vulnerability Scanning

Control Techniques and Suggested Audit Procedures for Critical Element SM-5

Table 11. Control Techniques and Suggested Audit Procedures for Critical Element SM-5: Monitor the effectiveness of the security program

Control activities	Control techniques	Audit procedures
SM-5.1. The effectiveness of security controls are periodically assessed	SM-5.1.1. Appropriate monitoring and testing policies and procedures are documented.	Review testing policies and procedures. Determine if there is an overall testing strategy or plan.
	SM-5.1.2. Management routinely conducts vulnerability assessments and promptly corrects identified control weaknesses.	Interview officials who conducted the most recent agency/entity vulnerability assessment. Review the methodology and tools used, test plans and results obtained, and corrective action taken. Determine if testing is performed that complies with OMB and NIST certification and accreditation and other testing requirements. If appropriate, perform independent testing with the approval of management. Determine if identified control weaknesses are promptly corrected.
	SM-5.1.3. Management routinely conducts privacy impact assessments and promptly corrects identified control weaknesses.	Review privacy impact assessments, including the methodology, a sample of test plan, and related testing results.
	SM-5.1.4. The frequency and scope of security control testing is commensurate with risk.	Determine if control testing is based on risk.
	SM-5.1.5. Performance measures and compliance metrics monitor the security processes and report on the state of compliance in a timely manner.	Review agency/entity performance measures and compare to OMB's performance measures and NIST guidance.
	SM-5.1.6. An annual independent evaluation of the federal agency's information security program tests the effectiveness of the security policies, procedures, and practices.	Review the results of these annual evaluations for both FISMA and privacy reporting and any assessments of their adequacy and effectiveness.
	SM-5.1.7. Federal agencies report on the results of the annual independent evaluations to appropriate oversight bodies. Under OMB guidance, the head of each agency must submit security and privacy reports to OMB, which consolidates the information for a report to Congress. The Comptroller General must also periodically evaluate and report to Congress on the adequacy and effectiveness of agency information security policies and practices.	Evaluate the reporting process and identify any significant discrepancies between reports at each level and whether the reports agree with independent audit evaluations. Note that OMB has annual requirements for FISMA and privacy reporting.

Source: GAO.

Exposure Draft

Critical Element SM-6. Effectively Remediate Information Security Weaknesses

When weaknesses are identified, the related risks should be reassessed, appropriate corrective or remediation actions taken, and follow-up monitoring performed to make certain that corrective actions are effective. Procedures should be established to reasonably assure that all IS control weaknesses, regardless of how or by whom they are identified, are included in the entity's remediation processes. For each identified IS control weakness, the entity should develop and implement appropriate action plans and milestones. Action plans and milestones should be developed based on findings from security control assessments, security impact analyses, continuous monitoring of activities, audit reports, and other sources. When considering appropriate corrective actions to be taken, the entity should, to the extent possible, consider the potential implications throughout the entity and design appropriate corrective actions to systemically address the deficiency. Limiting corrective action only to identified deficiencies would not necessarily address similar weaknesses in other systems or applications or result in the most effective and efficient corrective action.

In addition to developing action plans and modifying written policies to correct identified problems, entities should test the implementation of the corrective actions to determine whether they are effective in addressing the related problems. Management should continue to periodically review and test such corrective actions to determine if they remain effective on a continuing basis. This is an important aspect of managers' risk management responsibilities.

FISMA specifically requires that agencywide information security programs include a "process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency." Further, agencies must report on the adequacy and effectiveness of the information security program and practices in annual reports to OMB, Congress, and GAO and in annual budget and management plans and reports. The latter include reporting a FISMA "significant deficiency" in information security as a material

Exposure Draft

weakness. Government Performance and Results Act performance plans must describe time periods and resources needed to effectuate a risk-based program.

SM-6 Related NIST SP-800-53 Controls
CA-5 Plan of Action and Milestones

Control Techniques and Suggested Audit Procedures for Critical Element SM-6

Table 12. Control Techniques and Suggested Audit Procedures for Critical Element SM-6: Effectively remediate information security weaknesses

Control activities	Control techniques	Audit procedures
SM-6.1. Information security weaknesses are effectively remediated.	SM-6.1.1. Management initiates prompt action to correct deficiencies. Action plans and milestones are documented.	Review recent POA&Ms, FMFIA reports and prior year audit reports and determine the status of corrective actions. The objective of this procedure in an IS controls audit being performed as part of a financial audit or data reliability assessment is generally limited to understanding management's POAM process and related controls to ensure the accuracy of the information in the POA&Ms, determining whether IS control weaknesses identified by the IS controls audit are included in the POA&Ms, and, if not, determining the cause.
	SM-6.1.2. Deficiencies are analyzed in relation to the entire agency/entity, and appropriate corrective actions are applied entitywide.	Evaluate the scope and appropriateness of corrective actions.
	SM-6.1.3. Corrective actions are tested and are monitored after they have been implemented and monitored on a continuing basis.	Determine if implemented corrective actions have been tested and monitored periodically.

Source: GAO.

Critical Element SM-7. Ensure that activities performed by external third parties are adequately secure

Appropriate policies and procedures should be developed, implemented, and monitored to ensure that the activities performed by external third parties (for example, service bureaus, contractors, other service providers such as system development, network management, and security management) are documented, agreed to, implemented, and monitored for compliance. These should include

Exposure Draft

provisions for (1) security clearances (where appropriate and required), (2) background checks, (3) required expertise, (4) confidentiality/nondisclosure agreements, (5) security roles and responsibilities, (6) connectivity agreements, (7) individual accountability (for example, expectations, remedies), (8) audit access and reporting, (9) termination procedures, and (10) security awareness training. In addition, checks should be performed to periodically ensure that the procedures are being correctly applied and consistently followed, including the security of relevant contractor systems. Appropriate controls also need to be applied to outsourced software development.

FISMA information security requirements apply not only to information systems used or operated by an agency but also to information systems used or operated by a contractor of an agency or other agency on behalf of an agency. In addition, the Federal Acquisition Regulation (FAR) requires that federal agencies prescribe procedures for ensuring that agency planners on information technology acquisitions comply with the information technology security requirements of FISMA, OMB's implementing policies including Appendix III of OMB Circular A-130, and guidance and standards from NIST.⁵⁶ For example, NIST SP 800-35 *Guide to Information Technology Security Services* provides guidance pertaining to the acquisition or outsourcing of dedicated information system security services such that (1) incident monitoring, analysis, and response; (2) operation of information system security devices (for example, firewalls); and (3) key management services are supported by a risk assessment and approved by the appropriate, designated agency official. Acquisition or outsourcing of information system services explicitly addresses government, service provider, and end-user security roles and responsibilities.

Governmental and private entities face a range of risks from contractors and other users with privileged access to their systems,

⁵⁶ The FAR was established to codify uniform policies for acquisition of supplies and services by executive agencies. The FAR appears in the Code of Federal Regulations at 48 CFR Chapter 1.

Exposure Draft

applications and data. Contractors that provide systems and services or other users with privileged access to agency/entity systems, applications, and data can introduce risks to their information and systems; for example, contractors often provide unsupervised remote maintenance and monitoring of agency/entity systems. Contractor risks to people, processes, and technology are summarized in table 13.

Table 13. Examples of Agency-Identified Risks to Federal Systems and Data Resulting from Reliance on Contractors

Category	Risk description
People	Unauthorized personnel having physical access to agency IT resources (including systems, applications, facilities, and data).
	Unauthorized personnel having electronic access to agency IT resources (including systems, applications, and data).
	Increased use of foreign nationals.
	Contractor or privileged users of federal data and systems who may not receive appropriate, periodic background investigations.
	Inadequate segregation of duties (for example, software developer is the same individual who puts the software into production).
Processes	Failure by contractor or privileged users of federal data and systems to follow agency IT security requirements.
	Possible disclosure of agency-sensitive information to unauthorized individuals or entities.
	Lack of effective compliance monitoring of contractors performing work off-site or privileged users of federal data and systems.
	Contractor or privileged users of federal data and systems may have ineffective patch management processes.
Technology	Incorporation of unauthorized features in customized application software. For example, a third-party software developer has the potential to incorporate "back doors," spyware, or malicious code into customized application software that could expose agency IT resources to unauthorized loss, damage, modification, or disclosure of data.
	Encryption technology may not meet federal standards.
	Intentional or unintentional introduction of viruses and worms.

Source: Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk (GAO-05-362, April 2005).

Note: The various risks identified could represent multiple risks (i.e., risks in one or more of the identified categories of people, processes, and technology).

In addition to the risks identified in the table, there are specific risks from contractor software development activities and off-site operations. These risks include a poor patch management process that could impact entity operations (for example, entity Web sites),

Exposure Draft

a hosting infrastructure that may not separate customer and company data, and inadequate oversight at an off-site facility.

SM-7 Related NIST SP-800-53 Controls
 AC-20 Use of External Information Systems
 MA-4 Remote Maintenance
 PS-7 Third-Party Personnel Security
 SA-9 External Information System Services

Control Techniques and Suggested Audit Procedures for Critical Element SM-7

Table 14. Control Techniques and Suggested Audit Procedures for Critical Element SM-7: Ensure that activities performed by external third parties are adequately secure

Control activities	Control techniques	Audit procedures
SM-7.1. External third party activities are secure, documented, and monitored.	SM-7.1.1. Appropriate policies and procedures concerning activities of external third parties (for example, service bureaus, contractors, other service providers such as system development, network management, security management) are documented, agreed to, implemented, and monitored for compliance and include provisions for <ul style="list-style-type: none"> • clearances, • background checks, • required expertise, • confidentiality agreements, • security roles and responsibilities, • connectivity agreements, • expectations, • remedies, • audit access/audit reporting, • termination procedures, and • security awareness training. 	Review policies and procedures pertaining to external third parties for the entitywide, system, and application levels. Identify use of external third parties and review activities including compliance with FISMA, and applicable policies and procedures. See NIST SP 800-35 for guidance on IT security services. Determine how security risks are assessed and managed for systems operated by a third party. Determine whether external third party services that relate to the technology are adequately controlled. Coordinate assessment of security awareness training with SM-4.
	SM-7.1.2. Security requirements are included in the information system acquisition contracts based on an assessment of risk.	Review security provisions of selected contracts and determine that requirements are implemented. See FAR requirements for acquisition plans (48 CFR 7.1, 7.103 (u).

Source: GAO.

Exposure Draft

3.2. Access Controls (AC)

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure. Such controls include both logical and physical controls. Logical access controls require users⁵⁷ to authenticate themselves (through the use of secret passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions that they can execute. Physical access controls involve restricting physical access to computer resources and protecting them from intentional or unintentional loss or impairment. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users can intentionally or unintentionally read, add, delete, or modify data or execute changes that are outside their span of authority.

Access control policies and procedures should be formally developed, documented, disseminated, and periodically updated. Policies should address purpose, scope, roles, responsibility, and compliance issues; procedures should facilitate the implementation of the policy and associated access controls. NIST SP 800-12 provides guidance on security policies and procedures. It is fundamental that control techniques for both logical and physical access controls be risk-based. Access control policies and procedures and risk assessments are covered in section 3.1 of the manual.

For access controls to be effective, they should be properly authorized, implemented, and maintained. First, an entity should analyze the responsibilities of individual computer users to determine what type of access (for example, read, modify, delete)

⁵⁷ As used herein, users include those given any level of authorized access to computer resources, including business process application users, system administrators, etc.

Exposure Draft

users need to fulfill their responsibilities. Then, specific control techniques, such as specialized access control software, should be implemented to restrict access to these authorized functions alone. Such software can be used to limit a user's activities associated with specific systems or files and keep records of individual users' actions on the computer. Finally, access authorizations and related controls should be monitored, maintained, and adjusted on an ongoing basis to accommodate new and departing employees and changes in users' responsibilities and related access needs.

Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data. The following examples illustrate the potential consequences of such vulnerabilities.

- By obtaining direct logical access to data files, an individual could make unauthorized changes for personal gain or obtain sensitive information. For example, a person could (1) alter the address of a payee and thereby direct a disbursement to himself or herself, (2) alter inventory quantities to conceal a theft of assets, (3) alter critical data needed to make a strategic policy decision, or (4) obtain confidential personal, commercial, and governmental information.
- By obtaining logical access to business process applications⁵⁸ used to process transactions, an individual could grant unauthorized access to the application, make unauthorized changes to these programs, or introduce malicious programs, which, in turn, could be used to access data files, resulting in situations similar to those just described, or the processing of unauthorized transactions. For example, a person could alter a payroll or payables program to inappropriately generate a check for him/herself.
- By obtaining access to system-level resources, an individual could circumvent security controls to read, add, delete, or modify

⁵⁸ A computer program designed to help perform a business function such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements.

Exposure Draft

critical or sensitive business information or programs. Further, authorized users could gain unauthorized privileges to conduct unauthorized actions or to circumvent edits and other controls built into the application programs.

- By obtaining physical access to computer facilities and equipment, an individual could (1) obtain access to terminals or telecommunications equipment that provide input into the computer, (2) obtain access to confidential or sensitive information on magnetic or printed media, (3) substitute unauthorized data or programs, or (4) steal or inflict malicious damage on computer equipment and software.

The objectives of limiting access are to ensure that

- outsiders (for example, hackers) cannot gain unauthorized access to the agency's systems or data;
- authorized users have only the access needed to perform their duties;
- access to very sensitive resources, such as operating systems and security software programs, are limited to very few individuals;
- employees/contractors are restricted from performing incompatible functions or functions beyond their responsibility. (Segregation of duties is discussed in greater detail in section 3.4.)

If these objectives are met, the risk of inappropriate modification or disclosure of data can be reduced without interfering with users' practical needs. However, establishing the appropriate balance between user needs and security requires a careful analysis of the criticality and sensitivity of information resources available and the tasks performed by users. Access controls also apply to alternate work sites (for example, employee residence or contractor facility).

Implementing adequate access controls involves first determining what level and type of protection is appropriate for individual resources based on a risk assessment and on who needs access to these resources. These tasks should be performed by the resource owners. For example, program managers should determine how

Exposure Draft

valuable their program data resources are and what access is appropriate for personnel who must use an automated system to carry out, assess, and report on program operations. Similarly, managers in charge of systems development and modification should determine the sensitivity of hardware and software resources under their control and the access needs of systems analysts and programmers, and system administration officials should determine the access needs of their personnel. Levels of access granted to information resources should be consistent with FIPS 199 risk levels.

This section defines a set of critical elements that should be considered when conducting a comprehensive assessment of access controls. Today's networks and control environments are highly diverse, complex, and interconnected. Devices that are interconnected develop control dependencies (discussed in Chapter 2), directly and indirectly, on other devices such as routers, firewalls, switches, domain name servers, Web servers, network management stations, e-mail systems, and browser software. Audit objectives that are limited to targeted assessments such as a UNIX or Windows audit may not fully recognize the control dependencies on these systems.

Unfortunately, there are no simple solutions to controlling logical access. Each entity decides what combination of technologies to deploy and to what degree, based on business needs and priorities, risk management, and other factors. For instance, an entity may decide not to require users to periodically change passwords for e-mail because initial entry to the system relies on a two-factor token-based authentication system. Other entities may rely less on boundary protection but place more emphasis on audit and monitoring. Accordingly, the collection of controls used will vary from entity to entity.

The six critical elements for access controls are described here.

- *Boundary Protection.* Boundary protection pertains to the protection of a logical or physical boundary around a set of information resources and implementing measures to prevent unauthorized information exchange across the boundary in either

Exposure Draft

direction. Firewall devices represent the most common boundary protection technology at the network level

- *Identification and authentication.* If logical connectivity is allowed, then the users, processes acting on behalf of users, services, and specific devices are identified and authenticated by the information system. For example, users' identities may be authenticated through something they know (a traditional password), something they have (such as a smart card), or something about them that identifies them uniquely (such as a fingerprint).
- *Authorization.* If authentication is successful, authorization determines what users can do; i.e., it grants or restricts user, service, or device access to various network and computer resources based on the identity of the user, service, or device.
- *Sensitive system resources.* Controls over sensitive system resources are designed to ensure the confidentiality, integrity, and availability of system data such as passwords and keys during transmission and storage. Technologies used to control sensitive data include encryption, certificate management, hashing, checksums, and steganography.⁵⁹
- *Audit and monitoring.* Audit and monitoring control involves the collection, review, and analysis of auditable events for indications of inappropriate or unusual activity. These controls should be used to routinely assess the effectiveness of information security controls, perform investigations during and after an attack, and recognize an ongoing attack.
- *Physical security.* Physical security controls restrict physical access or harm to computer resources and protect these resources from intentional or unintentional loss or impairment. Such controls include guards, gates, and locks, and also environmental controls such as smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies.

⁵⁹Steganography is a technique that hides the existence of a message (for example, by embedding it within another message) and may be used where encryption is not permitted or to hide information in an encrypted file in case the encrypted file is deciphered. Other uses include digital watermarking and fingerprinting of audio and video files.

Exposure Draft

Although the primary relevance of these concepts is to access controls, they are also relevant to other areas, such as security management and configuration management. For example, configuration management assurance controls help ensure that network devices are configured and are operating as intended. This would include verifying operational patch levels, disabling unnecessary and dangerous services, correcting poorly configured services, and protecting against viruses and worms. Also, these concepts are relevant to activities such as periodic self-assessment programs (covered in Section 3.1, Security Management).

Assessing access controls involves evaluating the agency's success in performing each of the critical elements listed in Table 15. When evaluating control techniques and performing audit procedures for access controls, the auditor considers access to networks, access to operating systems, and access to infrastructure applications.⁶⁰

Table 15. Critical Elements for Access Control

Number	Description
AC-1.	Adequately protect information system boundaries
AC-2.	Implement effective identification and authentication mechanisms
AC-3.	Implement effective authorization controls
AC-4.	Adequately protect sensitive system resources
AC-5.	Implement an effective audit and monitoring capability
AC-6.	Establish adequate physical security controls

Source: GAO

Critical Element AC-1. Adequately protect information system boundaries

Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from network connected devices. At the entitywide level, access control policy is developed and promulgated through procedures, manuals, and other guidance. At the system level, any connections to the Internet, or to other external and internal networks or information systems, should occur through controlled interfaces (for example, proxies,

⁶⁰Infrastructure applications include databases, e-mail, browsers, plug-ins, utilities, and other applications.

Exposure Draft

gateways, routers and switches, firewalls, and concentrators). At the host or device level, logical boundaries can be controlled through inbound and outbound filtering provided by access control lists and personal firewalls. At the application level, logical boundaries to business process applications may be controlled by access control lists in security software or within the applications.

Implementing multiple layers of security to protect information system internal and external boundaries provides Defense-in-Depth(described earlier in Additional IS Risk Factors). According to security experts, a best practice for protecting systems against cyber attacks is for entities to build successive layers of defense mechanisms at strategic points in their information technology infrastructures. By using the strategy of Defense-in-Depth, entities can reduce the risk of a successful cyber attack. For example, multiple firewalls could be deployed to prevent both outsiders and trusted insiders from gaining unauthorized access to systems: one firewall could be deployed at the network's Internet connection to control access to and from the Internet, while another firewall could be deployed between wide area networks and local area networks to limit employees' access.

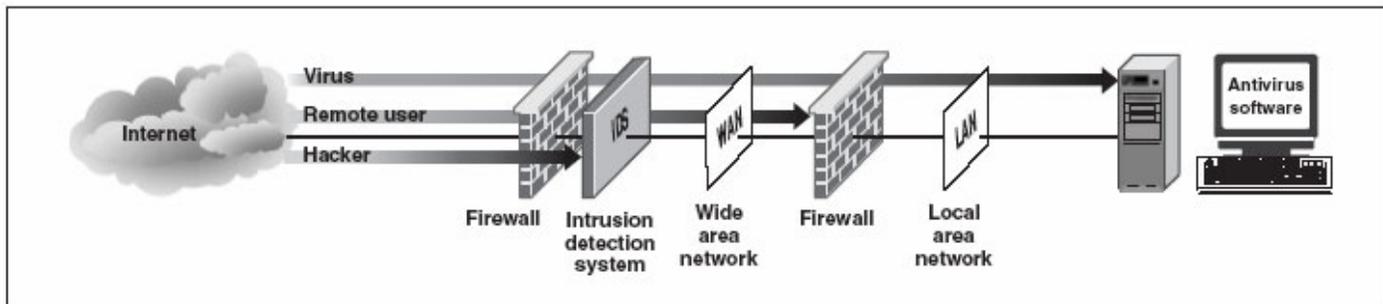
In addition to deploying a series of security technologies at multiple layers, deploying diverse technologies at different layers also mitigates the risk of successful cyber attacks. If several different technologies are deployed between the adversary and the targeted system, the adversary must overcome the unique obstacle presented by each of the technologies. For example, firewalls and intrusion detection technologies can be deployed to defend against attacks from the Internet, and antivirus software can be used to provide integrity protection for data transmitted over the network. Thus, Defense-in-Depth can be effectively implemented through multiple security measures among hosts, local area networks and wide area networks, and the Internet.

Defense-in-Depth also entails implementing an appropriate network configuration, which can, in turn, affect the selection and implementation of cybersecurity technologies. For example, configuring the agency's network to channel Internet access through a limited number of connections improves security by reducing the

Exposure Draft

number of points that can be attacked from the Internet. At the same time, the entity can focus technology solutions and attention on protecting and monitoring the limited number of connections for unauthorized access attempts. Figure 4 depicts how applying a layered approach to security through deploying both similar and diverse cybersecurity technologies at multiple layers can deflect different types of attacks.

Figure 4. Layered Approach to Network Security



Source: GAO analysis and Corel Draw.

Note: Excerpt from GAO, *Technologies to Secure Federal Systems*, GAO-04-467 (Washington, D.C.: March 2004).

AC-1.1. Appropriately control connectivity to system resources

Users obtain access to data files and software programs through one or more access paths through the networks and computer hardware and software. Accordingly, to implement an appropriate level of security, it is important that the entity, to the extent possible, identify, document, and control all access paths. Further, connectivity between systems should be approved only when appropriate by entity management. Consideration should be given to the risk and corresponding safeguards needed to protect sensitive data. NIST SP 800-47 provides guidance on interconnecting information systems.

Networks should be appropriately configured to adequately protect access paths between systems and consider the existing technologies. For standalone computers, identifying access paths may be relatively simple. However, in a networked environment, careful analysis is needed to identify all of the system's entry points

Exposure Draft

and paths to sensitive files. Networked systems typically consist of multiple personal computers that are connected to each other and to larger computers, such as file servers or mainframe processors. Many allow remote access (for example, dial-up, wireless, Internet) to the information systems from virtually any remote location. As a result, the entry points to the system can be numerous. Also, once the system has been entered, the programs available may provide multiple paths to various data resources and sensitive applications. Consequently, it is very important that all access paths be appropriately controlled and protected based on risk.

It is critical that access paths are identified as part of a risk analysis and documented in an access path diagram or similar network schematic. Such a diagram or schematic identifies the users of the system, the type of device from which they can access the system, the software used to access the system, the resources they may access, the system on which these resources reside, and the modes of operation and telecommunications paths. The goal in identifying access paths is to assist in identifying the points from which system resources could be accessed and the data stored—points that, therefore, must be controlled. Specific attention should be given to “backdoor” methods of accessing data by operators and programmers. As with other aspects of risk analysis, the access path diagram should be reviewed and updated whenever any changes are made to the system or to the nature of the program and program files maintained by the system.

If entry points and access paths are not identified, they may not be adequately controlled and may be exploited by unauthorized users to bypass existing controls to gain access to sensitive data, programs, or password files. Should this happen, managers will have an incomplete understanding of the risks associated with their systems and, therefore, may make erroneous risk management decisions.

Connecting to the Internet presents a multitude of vulnerabilities for an entity due to the Internet’s potential access to billions of people worldwide. Some Internet users are motivated to try to penetrate connected systems and have sophisticated software tools as aids, such as to repeatedly attempt access using different passwords. A

Exposure Draft

variety of specialized software and hardware is available to limit access by outside systems or individuals through telecommunications networks. Examples of network components that can be used to limit access include secure gateways (firewalls) that restrict access between networks (an important tool to help reduce the risk associated with the Internet); teleprocessing monitors, which are programs incorporated into the computer's operating system that can be designed to limit access; and communications port protection devices, such as a security modem that requires a password from a dial-in terminal before establishing a network connection. Also available is the smart card, a device about the size of a credit card that contains a microprocessor, which can be used to control remote access to a computer with authenticating information generated by the microprocessor and communicated to the computer. Encryption is often used to protect the confidentiality of remote access sessions and is extremely important to protecting wireless access to information systems.

Information systems may identify and authenticate specific devices before establishing a connection. Device authentication typically uses either shared known information (for example, media access control or transmission control program/Internet protocol addresses) or an organizational authentication solution to identify and authenticate devices on local and wide area networks. Thus, it is important for the auditor to identify the controls over devices that provide this type of protection.

Emerging threats from the Internet (for example, spam and spyware) require new and updated protection mechanisms. The entity should employ spam and spyware protection mechanisms at critical information system entry points (for example, firewalls, electronic mail servers, remote access servers) and at workstations, servers, or mobile computing devices on the network. Consideration should be given to using spam and software protection products from multiple vendors (for example, using one vendor for boundary devices and another vendor for workstations) to provide additional layers of defense. It is also important to centrally manage spam and software protection mechanisms and to have the system automatically update these mechanisms.

Exposure Draft

Depending on how access control techniques and devices are implemented, they can be used to

- verify terminal identifications to restrict access through specific terminals,
- verify IDs and passwords for access to specific applications,
- control access between telecommunications systems and terminals,
- restrict an application's use of network facilities,
- automatically disconnect at the end of a session,
- provide network activity logs that can be used to monitor network use and configuration,
- allow authorized users to shut down network components,
- monitor dial-in access to the system by monitoring the source of calls or by disconnecting and then dialing back users at preauthorized phone numbers,
- restrict in-house access to communications software,
- control changes to communications software, and
- restrict and monitor access to telecommunications hardware or facilities.

As with other access controls, to be effective, remote access controls should be properly implemented in accordance with authorizations that have been granted. In addition, tables or lists used to define security limitations should be protected from unauthorized modification, and in-house access to communications security software should likewise be protected from unauthorized access and modification. Dial-in phone numbers should not be published, and should be changed periodically.

An understanding of the system and network configurations and the control techniques that have been implemented is necessary to assess the risks associated with external access through telecommunications networks and the effectiveness of related controls. This is likely to require assistance from an auditor with special expertise in communications-related controls.

Exposure Draft

Connectivity should only be approved when appropriate to perform assigned official duties. Significant threats are posed by portable and mobile devices and personally owned information systems. Portable and mobile devices (for example, notebook computers, workstations, personal digital assistants) should not be allowed access to entity networks without first complying with security policies and procedures. Security policies and procedures might include activities such as scanning the devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (for example, wireless). Security controls include

- usage restrictions and implementation guidance,
- authorization by appropriate organizational officials, and
- documentation and monitoring of device access to entity networks.

The entity should also establish strict terms and conditions for the use of personally-owned information systems. The terms and conditions should address, at a minimum: (1) the types of applications that can be accessed from personally-owned information systems; (2) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (3) how other users of the personally-owned information system will be prevented from accessing federal information; (4) the use of virtual private networking and firewall technologies; (5) the use of and protection against the vulnerabilities of wireless technologies; (6) the maintenance of adequate physical security controls; (7) the use of virus and spyware protection software; and (8) how often the security capabilities of installed software are to be updated (for example, operating system and other software security patches, virus definitions, firewall version updates, spyware definitions).

Exposure Draft

AC-1.2. Appropriately control network sessions

It is desirable that information systems prevent further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users should be able to directly initiate session-lock mechanisms. The information system may also activate session-lock mechanisms automatically after a specified period of inactivity defined by the entity. A session lock is not, however, a substitute for logging out of the information system. When connectivity is not continual, network connections should automatically disconnect at the end of a session. OMB Memorandum M-06-16⁶¹ requires that all federal agencies use a “time-out” function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity.

In addition to technical controls, the initial screen viewed by an individual accessing an agency’s systems through a telecommunications network should provide a warning banner to discourage unauthorized users from attempting access, and make it clear that unauthorized browsing will not be tolerated. For example, an opening warning screen should state that the system is for authorized users only and that activity will be monitored. The information system should also display the agency’s privacy policy before granting access. Previous logon notification is another control that can identify unauthorized access. The information system notifies the user on successful logon, of the date and time of the last logon, the location of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

⁶¹ OMB, *Protection of Sensitive Agency Information* (Washington, D.C.: June 23, 2006).

Exposure Draft

<p><u>AC-1 Related NIST SP-800-53 Controls</u> AC-4 Information Flow Enforcement AC-8 System use Notification AC-9 Previous Logon Notification AC-11 Session Lock AC-12 Session Termination AC-17 Remote Access AC-18 Wireless Access Restrictions AC-19 Access Control for Portable and Mobile Devices CA-3 Information System Connections SC-7 Boundary Protection SC-10 Network Disconnect</p>

Control Techniques and Suggested Audit Procedures for Critical Element AC-1

Table 16. Control Techniques and Suggested Audit Procedures for Critical Element AC-1: Adequately protect information system boundaries

Control activity	Control techniques	Audit procedures
AC-1.1. Appropriately control connectivity to system resources.	AC-1.1.1. Connectivity, including access paths and control technologies between systems and to internal system resources, is documented, approved by appropriate entity management, and consistent with risk.	Review access paths in network schematics, interface agreements, systems documentation, and in consultation with IT management and security personnel identify control points; determine whether the access paths and related system documentation is up-to-date, properly approved by management, and consistent with risk assessments.
	AC-1.1.2. Networks are appropriately configured to adequately protect access paths within and between systems, using appropriate technological controls (e.g. routers, firewalls, etc.)	Interview the network administrator; determine how the flow of information is controlled and how access paths are protected. Identify key devices, configuration settings, and how they work together.

Exposure Draft

Control activity	Control techniques	Audit procedures
		<p>Perform security testing by attempting to access and browse computer resources including critical files, security software, and the operating system. These tests may be performed as (1) an “outsider” with no information about the agency’s computer systems, (2) an “outsider” with prior knowledge about the systems—for example, an ex-insider, and (3) an “insider” with and without specific information about the agency’s computer systems and with access to the agency’s facilities. Note: Due to the highly technical nature of such testing, it should be performed by persons possessing the necessary technical skills (e.g., an IT specialist). See Appendix V for additional information on the Knowledge, Skills, and Abilities needed to perform IS control audits.</p> <p>When performing insider tests, use an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, try to access the agency’s computer resources using default/generic IDs with easily guessed passwords. See NIST SP 800-42 for more details.</p> <p>When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, wireless, local area network, wide area network, and the Internet. See NIST SP 800-42 for more details.</p>
	AC-1.1.3. The information system identifies and authenticates specific network devices before establishing a connection. (for example, Media Access Control (MAC) or TCP/IP addresses).	When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, wireless, local area network, wide area network, and the Internet. See NIST SP 800-42 for more details.
	AC-1.1.4. Remote dial-up access is appropriately controlled and protected.	Interview network administrator and users; determine how remote dial-up access is controlled and protected (for example, monitor the source of calls and dial back mechanism); identify all dial-up lines through automatic dialer software routines and compare with known dial-up access; discuss discrepancies with management.

Exposure Draft

Control activity	Control techniques	Audit procedures
	AC-1.1.5. Remote Internet access is appropriately controlled and protected.	Interview network administrator and users; determine how connectivity is controlled and protected. Determine if federal agency policies, procedures, and practices comply with NIST SP 800-63 guidance on remote electronic authentication. Supplement with appropriate assessments in NIST 800-53A.
	AC-1.1.6. Remote wireless access is appropriately controlled and protected.	Interview network administrator and users; determine how connectivity is controlled and protected. Refer to NIST SP 800-97 <i>Establishing Wireless Robust Security Networks: A guide to IEEE.802.11i</i> for additional security assessment guidance. Test and validate entity controls: (1) use a wireless sniffer to capture data (for example, service set IDs (SSID)), (2) if an SSID is obtained, associate the SSID to the access point, (3) identify what network resources are available, (4) determine if a security protocol ⁶² such as wired equivalent privacy (WEP) is implemented, and (5) if a security protocol is used, employ a program to test the strength of the encryption algorithm. Test and validate entity controls to identify rogue wireless access points. Test for rogue wireless access points.
	AC-1.1.7. Connectivity is approved only when appropriate to perform assigned official duties. This includes portable and mobile devices, and personally-owned information systems.	Interview network administrator and users; review justifications for a sample of connections. Determine if these systems use appropriate safeguards such as automatic updates for virus protection and up-to-date patch protection, etc.
AC-1.2. Appropriately control network sessions.	AC-1.2.1. The information system prevents further access to the system by initiating a session lock, after a specified period of inactivity that remains in effect until the user reestablishes access using identification and authentication procedures.	Observe whether the system automatically initiates a session lock during a period of inactivity, and how the user can directly initiate a session lock, and then unlock the session.
	AC-1.2.2 Where connectivity is not continual, network connection automatically disconnects at the end of a session.	Interview network administrator and users; observe whether the control is implemented.

⁶².The optional cryptographic confidentiality algorithm specified by IEEE 802.11 used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance confidentiality

Exposure Draft

Control activity	Control techniques	Audit procedures
	AC-1.2.3. Appropriate warning banners are displayed before logging onto a system <ul style="list-style-type: none">• system use notification (for example, U. S. Government system, consent to monitoring, penalties for unauthorized use, privacy notices)• previous logon notification (for example, date and time of last logon and unsuccessful logons).	Interview network administrator and users; observe whether the control is fully implemented and complies with NIST guidance.

Source: GAO.

Critical Element AC-2. Implement effective identification and authentication mechanisms

Users (or processes on behalf of users), and devices should be appropriately identified and authenticated through the implementation of adequate logical access controls. User authentication establishes the validity of a user's claimed identity, typically during access to a system or application (for example, login). Users can be authenticated using mechanisms such as requiring them to provide something they have (such as a smart card); something they alone know (such as a password or personal identification number); or something that physically identifies them uniquely (such as a biometric fingerprint or retina scan). Logical controls should be designed to restrict legitimate users to the specific systems, programs, and files that they need, and prevent others, such as hackers, from entering the system at all.

At the entitywide level, information systems accounts need to be managed to effectively control user accounts and identify and authenticate users. Account management includes the identification of account types (i.e., individual, group, system), establishment of conditions for group membership, and assignment of associated authorizations. Resource owners should identify authorized users of the information system and specify access rights. Access to the information system should be granted based on a valid need to know that is determined by assigned official duties and should also consider proper segregation of duties. The entity should require proper identification for requests to establish information system accounts and approve all such requests. The entity should also specifically authorize and monitor the use of guest/anonymous accounts and remove, disable, or otherwise secure unnecessary accounts. Finally, the entity should ensure that account managers

Exposure Draft

are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured.

AC-2.1. Users are appropriately identified and authenticated

Identification and authentication is unique to each user (or processes acting on behalf of users). Account policies (for example, password policies, account lock out policies) should be formally established and enforced based on risk. Passwords, tokens, or other devices are used to identify and authenticate users. Identification is the process of distinguishing one user from all others, usually through user IDs. These are important because they are the means by which specific access privileges are assigned and recognized by the computer. However, the confidentiality of user IDs is typically not protected. For this reason, other means of authenticating users—that is, determining whether individuals are who they say they are—are typically implemented (for example, passwords, security tokens, etc.). In addition, the information system should limit the number of concurrent sessions for any user.

An entity may allow limited user activity without identification and authentication for publicly available information systems and Web sites. However, for actions without identification and authentication, management should consider the risk and only allow such actions to the extent necessary to accomplish mission objectives.

The most widely used means of authentication is through the use of passwords. However, passwords are not conclusive identifiers of specific individuals since they may be guessed, copied, overheard, or recorded and played back. Typical controls for protecting the confidentiality of passwords include the following:

- Individual users are uniquely identified rather than having users within a group share the same ID or password; generic user IDs and passwords should not be used.
- Passwords are not the same as user IDs.
- Password selection is controlled by the assigned user and not subject to disclosure.

Exposure Draft

- Passwords are changed periodically, about every 30 to 90 days. The more sensitive the data or the function, the more frequently passwords should be changed.
- Passwords are not displayed when they are entered.
- Passwords contain alphanumeric and special characters and do not use names or words that can be easily guessed or identified using a password-cracking mechanism.
- A minimum character length, at least 8 characters, is set for passwords so that they cannot be easily guessed.
- Use of old passwords (for example, within six generations) is prohibited.
- Vendor-supplied passwords such as SYSTEM, DEFAULT, USER, DEMO, and TEST, are replaced immediately on implementation of a new system.

To help ensure that passwords cannot be guessed, attempts to log on to the system with invalid passwords should be limited. Typically, potential users are allowed 3 to 7 attempts to log on. This, in conjunction with the use of pass phrases or other complex passwords, reduces the risk that an unauthorized user could gain access to a system by using a computer to try thousands of words or names until they found a password that provided access. NIST SP 800-63 provides guidance on password selection and content.

Another technique for reducing the risk of password disclosure is encrypting the password file. Encryption may be used to transform passwords into a form readable only by using the appropriate key, held only by authorized parties. Access to this file should be restricted to only a few people; encryption further reduces the risk that passwords could be accessed and read by unauthorized individuals. Passwords transmitted on the network may likewise be encrypted to prevent disclosure. Cryptographic controls and related audit procedures are covered in section AC-4.3.

In addition to passwords, identification devices such as ID cards, access cards, tokens, and keys may be used. Factors affecting the effectiveness of such devices include (1) the frequency that possession by authorized users is checked and (2) users' understanding that they should not allow others to use their

Exposure Draft

identification devices and should report the loss of such devices immediately. Procedures should also be implemented to handle lost or compromised passwords, access cards, or tokens. OMB Memorandum M-06-16 requires that federal agencies allow remote access to personally identifiable information and other sensitive information only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Also see AC-4.2.

A less common means of authentication is based on biometrics, an automated method of verifying or recognizing the identity of a person based on physiological or behavioral characteristics. Biometrics devices include fingerprints, retina patterns, hand geometry, speech patterns, and keystroke dynamics. Tests of biometric techniques include reviewing the devices, observing the operations, and taking whatever other steps may be necessary to evaluate their effectiveness, including obtaining the assistance of a specialist.

To further increase security, identification and authentication may be accomplished using any combination of multiple mechanisms such as a token ID in conjunction with a number, or a biometric reader in conjunction with a password (also known as multifactor identification). Management should implement effective procedures to determine compliance with authentication policies. Whatever technique is used, the implementation cost versus the risk and potential loss to the agency's operations from a breach in security should be taken into consideration.

Electronic signatures such as digital signatures and public key infrastructure (PKI) are used to identify the sender of information and ensure the integrity of critical information received from the sender. Several technologies such as personal identification numbers, smart cards, biometrics, or digital signatures (an encrypted set of bits that identify the user) can be used to create electronic signatures. The most common electronic signature in use today is the digital signature, which is unique to each individual and to each message. Digital signatures are used in conjunction with certificate authorities and other PKI encryption hardware, software, policies, and people to verify that the individuals on each end of a

Exposure Draft

communication are who they claim to be and to authenticate that nothing in the message has been changed. A digital certificate or shared secret may also be used to authenticate the identity of a device or devices involved in system communications, as opposed to the users.

In addition, appropriate session-level identification and authentication controls should be implemented, such as those related to name/address resolution service and the authenticity of communication sessions.

AC-2 Related NIST SP-800-53 Controls

AC-7 Unsuccessful Login Attempts

AC-10 Concurrent Session Control

AC-14 Permitted Actions Without Identification or Authentication

AU-10 Non-Repudiation

IA-2 User Identification and Authentication

IA-3 Device Identification and Authentication

IA-4 Identifier Management

IA-5 Authenticator Management

IA-6 Authenticator Feedback

SC-17 Public Key Infrastructure Certificates

SC-20 Secure Name/Address Resolution Service (Authoritative Source)

SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

SC-22 Architecture and Provisioning for Names/Address Resolution Service

SC-23 Session Authenticity

Exposure Draft

Control Techniques and Suggested Audit Procedures for Critical Element AC-2

Table 17. Control Techniques and Suggested Audit Procedures for Critical Element AC-2: Implement effective identification and authentication mechanisms

Control activity	Control techniques	Audit procedures
AC-2.1. Users are appropriately identified and authenticated.	AC-2.1.1. Identification and authentication is unique to each user (or processes acting on behalf of users), except in specially approved instances (for example, public Web sites or other publicly available information systems).	Review pertinent policies and procedures and NIST guidance pertaining to the authentication of user identities; interview users; review security software authentication parameters.
	AC-2.1.2. Account policies (including authentication policies and lockout policies) are appropriate given the risk, and enforced.	Review account policies and determine if they are based on risk and seem reasonable, based on interviews with system administrator and users. Determine how they are enforced, and test selected policies.
	AC-2.1.3. Effective procedures are implemented to determine compliance with authentication policies.	Review adequacy of procedures for monitoring compliance with authentication policies; selectively test compliance with key policies.
	AC-2.1.4. Selection of authentication methods (for example, passwords, tokens, biometrics, key cards, PKI certificates, or a combination therein) are appropriate, based on risk.	Determine whether authentication methods used are appropriate, based on risk.
	AC-2.1.5. Authenticators are unique for specific individuals, not groups; <ul style="list-style-type: none">• are adequately controlled by the assigned user and not subject to disclosure; and• cannot be easily guessed or duplicated. Additional considerations for passwords are described below.	Review pertinent entity policies and procedures; assess procedures for generating and communicating authenticators to users; interview users; review related security software parameters. Observe users using authenticators; attempt to logon without a valid authenticator. Assess compliance with NIST guidance on authenticator selection, content, and usage.
	AC-2.1.6. Password-based authenticators <ul style="list-style-type: none">• are not displayed when entered;• are changed periodically (e.g., every 30 to 90 days);• contain alphanumeric and special characters;• are sufficiently long (e.g., at least 8 characters in length);• have an appropriate minimum life (automatically expire);• are prohibited from reuse for a specified period of time (e.g., at least 6 generations); and• are not the same as the user ID.	Review pertinent entity policies and procedures; assess procedures for generating and communicating passwords to users; interview users; review security software password parameters. Observe users keying in passwords; attempt to logon without a valid password; make repeated attempts to guess passwords. Assess entity compliance with NIST SP 800-63, which provides guidance on password selection and content.

Exposure Draft

Control activity	Control techniques	Audit procedures
	AC-2.1.7. Attempts to log on with invalid passwords are limited (e.g., 3–7 attempts).	Examine security parameters for failed log-on attempts; review security logs to determine whether attempts to gain access are logged and reviewed by entity security personnel; if appropriate, repeatedly attempt to logon using invalid passwords.
	AC-2.1.8. Use of easily guessed passwords (such as names or words) are prohibited.	Review a system-generated list of current passwords; search password file using audit software to identify use of easily guessed passwords.
	AC-2.1.9. Generic user IDs and passwords are not used.	Interview users and security managers; review a list of IDs and passwords to identify generic IDs and passwords in use.
	AC-2.1.10. Vendor-supplied default passwords are replaced during installation.	Attempt to log on using common vendor-supplied passwords; search password file using audit software.
	AC-2.1.11. Passwords embedded in programs are prohibited. (Note: An embedded password is a password that is included into the source code of an application or utility. Applications often need to communicate with other applications and systems and this requires an “authentication” process which is sometimes accomplished through the use of embedded passwords).	Determine if passwords are embedded in programs and if this practice is explicitly prohibited.
	AC-2.1.12. Use of and access to authenticators is controlled (e.g., their use is not shared with other users).	Interview users. To evaluate biometrics or other technically sophisticated authentication techniques, the auditor may need to obtain the assistance of a specialist.
	AC-2.1.13. Effective procedures are implemented to handle lost, compromised, or damaged authenticators (e.g., tokens, PKI certificates, biometrics, passwords, and key cards).	Identify procedures for handling lost or compromised authenticators; interview users and selectively test compliance with procedures.
	AC-2.1.14. Concurrent sessions are appropriately controlled.	Review procedures for controlling and auditing concurrent logons from different workstations.
	AC-2.1.15. Where appropriate, digital signatures, PKI, and electronic signatures are effectively implemented.	Determine how nonrepudiation is assured and if PKI and electronic/digital signatures are effectively implemented.
	AC-2.1.16. PKI-based authentication <ul style="list-style-type: none"> validates certificates by constructing a certification path to an accepted trust anchor; establishes user control of the corresponding private key; and maps the authenticated identity to the user account. 	Review pertinent entity policies and procedures; assess procedures for generating and communicating certificates to users; interview users; review security software certificate parameters; obtain the help of experts if needed.
	AC-2.1.17. Authentication information is obscured (e.g., password is not displayed)	Review procedures for controlling the display of authentication information.
	AC-2.1.18. Appropriate session-level controls are implemented (e.g., name/address resolution service, session authenticity)	Assess the adequacy of session-level controls

Source: GAO.

Exposure Draft

Critical Element AC-3. Implement effective authorization controls

Once a user is authenticated, authorization⁶³ is used to allow or prevent actions by that user based on predefined rules. Authorization includes the principles of legitimate use, least privilege, and separation of duties (discussed in section 3.4). Operating systems have some built-in authorization features such as user rights and privileges, groups of users, and permissions for files and folders. Network devices, such as routers, may have access control lists that can be used to authorize users who can access and perform certain actions on the device. Access rights and privileges are used to implement security policies that determine what a user can do after being allowed into the system.

Access rights, also known as permissions, allow the user to look, read, or write to a certain file or directory. Privileges are a set of access rights permitted by the access control system. In a Microsoft Windows™ system, rights are what give the user or members of a group the access needed to perform management tasks or simply to access a system. Information system access permissions are a Unix term that describe the kind of access to files a user is granted. A set of permissions is associated with every file and directory that determines who can read it, write to it, or execute it. Only the owner of the file (or the super user⁶⁴) can change these permissions. Maintaining access rights, permissions, and privileges is one of the most important aspects of administering system security.

AC-3.1. User accounts are appropriately controlled

In order to adequately control user accounts, an entity should institute policies and procedures for authorizing logical access to information resources and document such authorizations. These policies and procedures should cover user access needed for routine operations, emergency access, and the sharing and disposition of data with individuals or groups outside the entity. Further, logical access controls should enforce segregation of duties.

⁶³Access privileges granted to a user, program, or process.

⁶⁴The term “super user” denotes the highest level of user privilege and can allow unlimited access to a system's file and set up.

Exposure Draft

The computer resource owner should identify the specific user or class of users authorized to obtain direct access to each resource for which they are responsible. Access should be limited to individuals with a valid business purpose (least privilege). Unnecessary accounts (default, guest accounts) should be removed, disabled, or otherwise secured. This process can be simplified by developing standard profiles, which describe access needs for groups of users with similar duties, such as accounts payable clerks.

The owner should also identify the nature and extent of access to each resource that is available to each user. This is referred to as the user's profile. In general, users may be assigned one or more of the following types of access to specific computer resources:

- read access—the ability to look at and copy data or a software program
- update access—the ability to change data or a software program
- delete access—the ability to erase or remove data or programs
- merge access—the ability to combine data from two separate sources
- execute access—the ability to execute a software program

Access may be permitted at the file, record, or field level. Files are composed of records, typically one for each item or transaction. Individual records are composed of fields that contain specific data elements relating to each record.

Owners should periodically review access authorization listings and determine whether they remain appropriate. Access authorizations should be documented on standard forms and maintained on file. Listings of authorized users and their specific access needs and any modifications should be approved by an appropriate senior manager and directly communicated in writing by the resource owner to the security management function. A formal process for transmitting these authorizations, including the use of standardized access request forms, should be established to reduce the risk of mishandling, alterations, and misunderstandings.

Exposure Draft

Security managers should review access authorizations for new or modified access privileges and discuss any questionable authorizations with the resource owners (authorizing officials).

Approved authorizations should be maintained on file. Compliance with access authorizations should be monitored by periodically comparing authorizations to actual access activity. Access control software typically provides a means of reporting user access authorizations and access activity. All changes to security access authorizations should be automatically logged and periodically reviewed by management independent of the security function. Unusual activity should then be investigated.

Broad or special access privileges, such as those associated with operating system software that allow normal controls to be overridden, are only appropriate for a small number of users who perform system maintenance or manage emergency situations. Such special privileges may be granted on a permanent or temporary basis. However, any such access should also be approved by a senior security manager, written justifications should be kept on file, and the use of highly sensitive files or access privileges should be routinely reviewed by management. Special access privileges, access to sensitive files, and related audit procedures are covered in section AC-4.1.

For systems that can be accessed through public telecommunications lines, some users may be granted dial-up access. This means that these individuals can use a modem to access and use the system from a remote location, such as their home or a field office. Because such access can significantly increase the risk of unauthorized access, it should be limited and the associated risks weighed against the benefits. To help manage the risk of dial-up access, justification for such access should be documented and approved by owners. (See section AC-1 for controls to help manage the risks of dial-up access, such as dial-back procedures to preauthorized phone numbers or the use of security modems, tokens, or smart cards to authenticate a valid user.)

Exposure Draft

Inactive accounts and accounts for terminated individuals should be disabled or removed in a timely manner. It is important to notify the security function immediately when an employee is terminated or, for some other reason, is no longer authorized access to information resources.

Notification may be provided by the human resources department or by others, but policies should exist that clearly assign responsibility for such notification. Terminated employees who continue to have access to critical or sensitive resources pose a major threat, as do individuals who may have left under acrimonious circumstances.

Owners should determine disposition and sharing of data. A mechanism should be established so that the owners of data files and programs determine whether and when these resources are to be maintained, archived, or deleted. Standard disposition forms can be used and maintained on file to document the users' approvals. In addition, resource owners should determine if, with whom, and by what means information resources can be shared. When files are shared with other entities, it is important that (1) data owners understand the related risks and approve such sharing and (2) receiving entities understand the sensitivity of the data involved and safeguard the data accordingly. This should require a written agreement before sensitive information is shared.

Required access to shared file systems should be restricted to the extent possible (for example, only to particular hosts, and only for the level of access required). Many scientific agencies, such as the National Aeronautics and Space Administration (NASA) and the National Institutes of Health (NIH) use file sharing networks. File sharing facilitates connections between persons who are looking for certain types of files. A type of file sharing known as peer-to-peer (P2P) refers to any software or system allowing individual users of the Internet to connect directly to each other and trade files. While there are many appropriate uses of this technology, several studies show that the vast majority of files traded on P2P networks are copyrighted music files and pornography. Data also suggest that P2P is a common avenue for the spread of computer viruses within IT systems. As required by FISMA, agencies are to use existing NIST standards and guidance to complete system risk and impact

Exposure Draft

assessments in developing security plans and authorizing systems for operation. Operational controls detailing procedures for handling and distributing information and management controls outlining rules of behavior for users should ensure that proper controls are in place to prevent and detect improper file sharing.⁶⁵

Emergency and temporary access authorization needs to be controlled. Occasionally, there will be a need to grant temporary access privileges to an individual who is not usually authorized access. Such a need may arise during emergency situations, when an individual is temporarily assigned duties that require access to critical or sensitive resources, or for service or maintenance personnel. In addition, contractor personnel may require temporary access while involved in systems development or other work. As with normal access authorizations, temporary access should be approved and documented and the related documentation maintained on file. Temporary user identifications and authentication devices, such as passwords, should be designed to automatically expire after a designated date. Also, management should periodically review emergency and temporary access accounts to determine that they are still necessary.

AC-3.2. Processes and services are adequately controlled

Only authorized processes and services should be permitted in information systems and they should be limited to what is essential to effectively perform an agency's mission and business functions. In an information system, processes are systematic sequences of operations to produce a specified result. This includes all functions performed within a computer such as editing, calculating, summarizing, categorizing, and updating. Services refer to "customer or product-related business functions" such as file transfer protocol (FTP), hypertext transfer protocol (HTTP), and mainframe supervisor calls. Each system provides a set of services. For example, a computer network allows its users to send packets to specified destinations; a database system responds to queries; and a processor performs a number of different instructions.

⁶⁵ OMB Memorandum M-04-26, *Personal Use Policies and "File Sharing" Technology*, (Washington, D.C.: September 8, 2004).

Exposure Draft

Controls related to processes and services include all of the technological and managerial safeguards established and applied to an information system to protect hardware, software, and data from accidental or malicious modification, destruction, or disclosure.

When evaluating an agency's processes and services, it is important to consider the following:

- available processes and services should be minimized,
- the functions and purposes of processes and services should be documented and approved by management, and
- information available to unauthorized users should be restricted.

Proper control of information system processes and services is critical to ensuring the confidentiality, integrity, and availability of user data and, ultimately, the accomplishment of an agency's mission. Access control policies and enforcement mechanisms are employed by entities to control access between users (or processes acting on behalf of users) and objects (for example, segments, devices, files, records, fields, processes, programs) in the information system. Access control policies can be identity-based, role-based, or rule-based.⁶⁶ Associated enforcement mechanisms include access control lists, access control matrices, and cryptography. Where encryption of stored information is used as an access enforcement mechanism, the cryptography used should be in compliance with applicable standards.

Configuring systems only for necessary capabilities minimizes processes and services. First, only required services should be installed. Second, the number of individuals with access to such services should be restricted based on the concept of least privilege; this means that users should have the least amount of privileges (access to services) necessary to perform their duties. Third, the use of information services needs to be monitored. Fourth, it is important to maintain current service versions. According to NIST

⁶⁶Identity-based access is based on the identities of users and information system resources. Role-based access is based on users' roles/responsibilities. Rule-based access is based on user or resource attributes and a predetermined rule set.

Exposure Draft

guidance, the information system should be periodically reviewed to identify and eliminate unnecessary services (for example, FTP, HTTP, mainframe supervisor calls) and protocols that would introduce an unacceptable level of risk should be disabled.⁶⁷ The information system that supports the server functionality should be, as much as possible, dedicated to that purpose. In addition, the function and purpose of processes and services should be documented and approved by appropriate entity officials.

According to NIST SP 800-53, additional process and service controls should be implemented to

- prohibit remote activation of collaborative computing mechanisms (e.g. video and audio devices),
- ensure that lower priority process do not interfere with higher priority processes, and
- ensure proprietary information and applications is protected from processes and systems available to the public.

<u>AC-3 Related NIST SP-800-53 Controls</u>

AC-2 Account Management

AC-3 Access Enforcement

AC-6 Least Privilege

CM-7 Least Functionality

SC-6 Resource Priority

SC-14 Public Access Protections

SC-15 Collaborative Computing

⁶⁷See NIST Special Publications (SP) 800-10 and 800-41 for information on configuring firewalls and filtering common protocols to minimize vulnerabilities from Internet services. SP 800-10, from 1994, contains basic information that is still applicable, but SP 800-41 updates the earlier document and covers Internet protocol packet filtering and more recent policy recommendations.

Exposure Draft

Control Techniques and Suggested Audit Procedures for Critical Element AC-3

Table 18. Control Techniques and Suggested Audit Procedures for Critical Element AC-3: Implement effective authorization controls

Control activity	Control techniques	Audit procedures
AC-3.1. User accounts are appropriately controlled.	AC-3.1.1. Resource owners have identified authorized users and the access they are authorized to have.	These audit procedures should be coordinated with section 3.4 (segregation of duties) to ensure that users do not have access to incompatible functions. Review written policies and procedures; for a selection of users (both application and information security personnel), review access authorization documentation and applicable rights and privileges in the information system.
	AC-3.1.2. Security administration personnel set parameters of security software to provide access as authorized and restrict access that has not been authorized. This includes access to data files, load and source code libraries (if applicable), security files, and operating system files. Standard naming conventions are established and used effectively as a basis for controlling access to data, and programs.	Determine directory names for sensitive or critical files and obtain security reports of related access rules. Using these reports, determine who has access to sensitive files and whether the access matches the level and type of access authorized. Determine whether standard naming conventions are established and used effectively.
	AC-3.1.3. Security managers review access authorizations and discuss any questionable authorizations with resource owners.	Interview security managers and review documentation provided to them.
	AC-3.1.4. All changes to security access authorizations are automatically logged and periodically reviewed by management independent of the security function; unusual activity is investigated.	Review a selection of recent changes to security access authorizations and related logs for evidence of management review and unusual activity; determine if unusual activity is being/has been investigated.
	AC-3.1.5. Resource owners periodically review access authorizations for continuing appropriateness.	Interview owners and review supporting documentation; determine whether inappropriate access rights are removed in a timely manner.
	AC-3.1.6. Access is limited to individuals with a valid business purpose (least privilege).	Identify who has access to user accounts and sensitive system resources and the business purpose for this access.
	AC-3.1.7. Unnecessary accounts (default, guest accounts) are removed, disabled, or otherwise secured.	Verify that unnecessary accounts are removed, disabled, or secured.
	AC-3.1.8. Inactive accounts and accounts for terminated individuals are disabled or removed in a timely manner.	Review security software parameters; review system-generated list of inactive logon IDs, and determine why access for these users has not been terminated. Obtain a list of recently terminated employees from Personnel and, for a selection, determine whether system access was promptly terminated.

Exposure Draft

Control activity	Control techniques	Audit procedures
	AC-3.1.9. Access to shared file systems are restricted to the extent possible (for example, only to particular hosts, and only for the level of access required).	Determine how access to shared file systems is restricted and verify that it works effectively.
	AC-3.1.10. Emergency or temporary access is appropriately controlled, including <ul style="list-style-type: none"> • documented and maintained, • approved by appropriate managers, • securely communicated to the security function, • automatically terminated after a predetermined period, and • all activity is logged. 	Review pertinent policies and procedures; compare a selection of both expired and active temporary and emergency authorizations (obtained from authorizing parties) with a system-generated list of authorized users. Determine the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed.
AC-3.2. Processes and services are adequately controlled.	AC-3.2.1. Available processes and services are minimized, such as through <ul style="list-style-type: none"> • installing only required processes and services based on least functionality, • restricting the number of individuals with access to such services based on least privilege, • monitoring the use of such services, and • maintaining current service versions. 	Review procedures for minimizing processes and services; interview system administrator; identify what services are installed and determine if they are required; determine who has access to these services and if they need them; determine how access to these services is monitored; and determine if the service versions are kept current. If appropriate, scan for poorly configured, unnecessary, and dangerous processes and services.
	AC-3.2.2. The function and purpose of processes and services are documented and approved by management.	Obtain documentation describing the function and purpose of processes and services, and evidence of management approval.
	AC-3.2.3. Information available to potential unauthorized users is appropriately restricted.	Determine if information about available processes and services is appropriately restricted.
	AC-3.2.4. The information system prohibits remote activation of collaborative computing mechanisms (for example, video and audio conferencing) and provides an explicit indication of use to the local users (for example, use of camera or microphone).	Determine if remote activation of collaborative computing services have been physically disconnected.
	AC-3.2.5. The information system limits the use of resources by priority. (Priority protection ensures that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.)	Interview the systems administrator and review appropriate systems documentation.
	AC-3.2.6. For publicly available systems, the information system controls protect the integrity and availability of the information and applications.	Identify controls used to protect the integrity and availability of the information and applications on such systems and test controls to ensure their effectiveness.

Source: GAO.

Critical Element AC-4. Adequately protect sensitive system resources

Certain system resources are more sensitive than others because, if compromised, serious security breaches could occur. Three areas

Exposure Draft

related to sensitive system resources are: (1) restricting and monitoring access, (2) implementing adequate media controls over sensitive data, and (3) where appropriate, implementing effective cryptographic controls. Such sensitive system resources include system software, system utilities, configuration management systems, file maintenance systems, security software, data communications systems, and database management systems. Restricting access to sensitive system resources such as system software and related documentation is critical to controlling the overall integrity of information systems. For example, if system software is not adequately protected, an individual could gain access to capabilities that would allow him or her to bypass security features found in either operating system security software or access controls built into application software. The individual would then be able to read, modify, or destroy application programs, master data files, and transaction data, and subsequently erase any electronic audit trail of his or her activities. In addition, inadequate media controls can result in a loss of confidentiality of sensitive data. Further, cryptographic controls may be needed to protect sensitive information where it is not otherwise possible or practical to adequately restrict access through either physical or logical access controls.

AC-4.1. Access to sensitive system resources is restricted and monitored

Access to sensitive system resources, such as system software and powerful system utilities, should be appropriately restricted and monitored. System software is a set of programs designed to operate and control the processing activities of computer equipment. Generally, one set of system software is used to support and control a variety of applications that may run on the same computer hardware. System software helps control and coordinates the input, processing, output, and data storage associated with all of the applications that run on a system. Some system software can change data and program code on files without leaving an audit trail. The following are examples of system software:

- operating system software
- system utilities
- configuration management systems

Exposure Draft

- file maintenance software
- security software
- data communications systems
- database management systems

Access to sensitive system resources should be restricted to individuals or processes that have a legitimate need for this access for the purposes of accomplishing a valid business purpose. For example, access to system software should be restricted to a limited number of personnel who have job responsibilities associated with the use of that software. Responsibilities for using system utilities should be clearly defined and understood by systems programmers. Application programmers and computer operators should be specifically prohibited from accessing system software. Justification and approval by appropriate entity officials for access to system software should be documented and retained. Appropriate entity officials should periodically review the use of privileged system software and utilities to ensure that access permissions correspond with position descriptions and job duties. Further, the use of sensitive/privileged accounts should be adequately monitored. Responsibilities for monitoring use should be clearly defined and understood by entity officials.

Typically, access to operating system software is restricted to a few systems programmers whose job it is to modify the system, when needed, and intervene when the system will not operate properly. In addition, database administrators need access to the system's database management system and a designated senior-level security administrator needs access to security software. However, application programmers and computer operators should not have access to system software, as this would be incompatible with their assigned responsibilities and could allow unauthorized actions to occur. (See section 3.4 for details on segregation of duties.)

The number of personnel authorized to access the system will vary depending on the size and needs of the entity and, therefore, should be determined based on an analysis of the agency's operations. For example, a large entity that must maintain operations on a 24-hour basis will need more operating systems analysts and programmers

Exposure Draft

than a smaller entity that operates on a less intensive schedule. There may be a tendency for entities to authorize access to many individuals so that emergency operating problems can be handled promptly. However, management should balance the need for efficiency with the need for security.

Because of the powerful capabilities at the disposal of those who have access to system software and related tools, use of the tools should be adequately controlled and monitored to identify any inappropriate or unusual behavior. Such behavior may indicate unauthorized access or an individual who is improperly exploiting access privileges. For example, greater than normal use of system software or use at odd hours may indicate that an individual is using the software to search for system weaknesses to exploit or to make unauthorized changes to system or application software or data. For monitoring to be effective in both detecting and deterring inappropriate use, personnel authorized to use system software should understand which uses are appropriate and which are not and also that their activities may be monitored. Such policies should be documented and distributed to all personnel.

Policies and techniques should be implemented for using and monitoring the use of system tools and utilities. Some system utilities are used to perform system maintenance routines that are frequently required during normal processing operations. Other utilities aid the development and documentation of applications systems. These utilities can aid individuals who have fraudulent or malicious intentions in understanding how the programs or data in an application system operate and in how to make unauthorized modifications.

Following is a listing of some utilities with their intended functions that could be misused without proper monitoring and control:

- Flowcharters, transaction profile analyzers, execution path analyzers, and data dictionaries can be used to understand application systems.
- Data manipulation utilities, data comparison utilities, and query facilities can be used to access and view data, with manipulation utilities also allowing data modification.

Exposure Draft

- Online debugging facilities permit online changes to program object code leaving no audit trail and can activate programs at selected start points.
- Library copiers can copy source code from a library into a program, text and online editors permit modification of program source code, and online coding facilities permit programs to be coded and compiled in an interactive mode.

To prevent or detect the misuse of systems utilities, policies should be clearly documented regarding their use. In addition, the use of utilities should be monitored. Generally, system software contains a feature that provides for logging and reporting of its use. Such reports should identify when and by whom the software was used. It is important that this software operation work properly and that the reports are reviewed on a regular basis.

The availability of standard usage data may assist the systems manager in identifying unusual activity. Some systems can be designed to compare standard usage data with actual use and report significant variances, thus making it easier for the system manager to identify unusual activity. When questionable activity is identified, it should be investigated. If improper activity is determined to have occurred, in accordance with security violation policies, the incident(s) should be documented, appropriate disciplinary action taken, and, when appropriate, higher-level management notified. Further, the possibility of damage or alteration to the system software, application software, and related data files should be investigated and corrective action taken if needed. Such action should include notifying the resource owner of the violation.

In addition to controlling access to sensitive system resources, it is also important to control a number of other activities. First, default permissions and rights to system software and network devices should be changed during installation. Second, system libraries should be appropriately controlled. For example, the migration of system software from the testing environment to the production environment may be performed, after approval, by an independent library control group. Outdated versions of system software should be removed from the production environment to preclude their use. Some changes may be made specifically to correct security or

Exposure Draft

integrity vulnerabilities, and using outdated versions allows the agency's data and systems to remain exposed to these vulnerabilities. Third, access to authentication services and directories should also be appropriately controlled. Finally, access to mobile code⁶⁸ (see next paragraph) should be appropriately controlled due to its potential to cause damage to the information system if used maliciously.

Mobile code refers to programs (for example, script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics. Being able to download files and electronic documents off the Internet is a useful function and a common practice today. Web pages serve as an electronic counterpart to paper documents; however, unlike paper documents, Web pages can entail active content that is capable of delivering digitally encoded multimedia information enlivened through embedded computer instructions. The popularity of the World Wide Web has spurred the trend toward active content. A dynamic weather map, a stock ticker, and live camera views or programmed broadcasts appearing on a Web page are common examples of the use of this technology. Like any technology, active content can provide a useful capability, but can also become a source of vulnerability for an attacker to exploit.

Mobile code controls should include registration, approval, and control procedures to prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. All mobile code or executable content employed should be registered unless otherwise approved by the authorizing official. Uploading of mobile code or executable content from one organizational information system to another should also be similarly authorized.

⁶⁸Mobile code is a software program or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. Examples of mobile code include scripts (JavaScript, VBScript), Java applets, Active X controls, and macros embedded within Office documents.

Exposure Draft

Sensitive system resources may be further protected by partitioning applications, isolating security functions, and establishing a trusted communication path. First of all, through application partitioning, the information system physically or logically separates user interface services (for example, public Web pages) from information storage and management services (for example, database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. Secondly, it is desirable for the information system to isolate security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (for example, address space) for each executing process. Thirdly, the information system should establish a trusted communication path between the user and the security functionality of the system. Technical experts may be needed to examine and test these controls. Finally, as appropriate, controls should be in place over information leakage through electromagnetic signals emanations.

AC-4.2. Adequate media controls have been implemented

Media controls should be implemented to control unauthorized physical access to digital and printed media removed from the information system and during pick up, transport, and delivery to authorized users. Media should also be properly labeled to identify its sensitivity and distribution limitations. Finally, all sensitive information should be removed from media before its disposal or transfer to another use.

As discussed in NIST SP 800-53, information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). Media controls also apply to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).

Exposure Draft

NIST SP 800-53 also states that an organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.

One sensitive area is the storage of personally identifiable information on portable media. The ability to store and transport substantial volumes of data on portable devices creates an additional exposure to information confidentiality. The entity should have adequate controls in place over such portable media. OMB Memorandum M-06-16 recommends federal agencies encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by the agency's Deputy Secretary or an individual they may designate in writing.

In addition, as part of the risk assessment process, entities should identify information that is sensitive, including personally identifiable information. Entities should implement controls to adequately protect the confidentiality of such information, including any copies of such data. OMB Memorandum M-06-16 recommends federal agencies to log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required. This OMB Memorandum provides additional guidance on controls over personally identifiable and other sensitive information. Also see AC-1.2 and AC-2.1.

Automated marking and labeling of information helps to enforce information security access policy. Information system outputs

Exposure Draft

should be marked using standard naming conventions to identify any special dissemination, handling, or distribution instructions. Similarly, information in storage, in process, and transmission should be appropriately labeled. Further, a means should be provided for the information system to ensure that the labels a user associates with information provided to the system are consistent with the information that the user is allowed to access. It is important that security parameters are exchanged between systems to authenticate services requested by another system. Security parameters include, for example, security labels and markings. Security parameters may be explicitly or implicitly associated with the information contained within the information system.

The entity should have policies and procedures in place to remove sensitive information⁶⁹ and software from computers, disks, and other equipment or media when they are disposed of or transferred to another use. Further, approved equipment and techniques should be used and periodically tested to ensure correct performance. If sensitive information is not fully cleared, it may be recovered and inappropriately used or disclosed by individuals who have access to the discarded or transferred equipment and media. The responsibility for clearing information should be clearly assigned. Also, standard forms or a log should be used to document that all discarded or transferred items are examined for sensitive information and that this information is cleared before the items are released.

AC-4.3. Cryptographic controls are effectively used

Where appropriate, cryptographic tools help provide access control by rendering data unintelligible to unauthorized users and/or protecting the integrity of transmitted or stored data. In some cases—especially those involving telecommunications—it is not possible or practical to adequately restrict access through either physical or logical access controls. In these cases, cryptographic tools can be used to identify and authenticate users and help protect

⁶⁹The process of removing sensitive information from computer media is often referred to as sanitization. It includes removing all labels, markings, and activity logs. NIST SP 800-36 provides guidance on appropriate sanitization equipment, techniques, and procedures.

Exposure Draft

the integrity and confidentiality of data and computer programs, both while these data and programs are “in” the computer system and while they are being transmitted to another computer system or stored on removable media.

As discussed in FIPS Pub 140-2, cryptographic-based security systems may be utilized in various computer and telecommunication applications (e.g., data storage, access control and personal identification, network communications, radio, facsimile, and video) and in various environments (e.g., centralized computer facilities, office environments, and hostile environments). The cryptographic services (e.g., encryption, authentication, digital signature, and key management) provided by a cryptographic module are based on many factors that are specific to the application and environment. The security level to which a cryptographic module is validated should be chosen to provide a level of security appropriate for the security requirements of the application and environment in which the module will be utilized and the security services that the module will provide. The security requirements for a particular security level include both the security requirements specific to that level and the security requirements that apply to all modules regardless of the level.

Cryptography involves the use of algorithms (mathematical formulae) and combinations of keys (strings of bits) to do any or all of the following:

- encrypt, or electronically scramble a message or file so that it is unintelligible to those who do not have the secret key needed to decrypt it, thus keeping the contents of the message or file confidential,
- provide an electronic signature that can be used to determine if any changes have been made to the related file, thus ensuring the file’s integrity, and
- link a message or document to a specific individual’s or group’s key, thus ensuring that the “signer” of the file can be identified.

Cryptographic tools are especially valuable for any application that involves “paperless” transactions or for which the users want to

Exposure Draft

avoid relying on paper documents to substantiate data integrity and validity. Examples include

- electronic commerce, where purchase orders, receiving reports, and invoices are created, approved, and transmitted electronically;
- travel administration, where travel orders and travel vouchers are created, approved, and transmitted electronically; and
- protection of documents or digital images, such as contracts, personnel records, or diagrams, which are stored on electronic media.

Cryptographic tools may be linked to an individual application or implemented so that they can be used to sign or encrypt data associated with multiple applications. For example, the personal computers connected to a local area network may each be fitted with hardware and/or software that identifies and authenticates users and allows them to encrypt, sign, and authenticate the messages and files that they send or receive, regardless of the application that they are using.

There are a number of technical issues to consider concerning cryptography. Some of the key considerations are listed here.

- Are the cryptographic tools implemented in software or through the use of a hardware module? (Hardware modules are generally more secure.)
- How is the data transmitted between the computer's memory and the cryptographic module, and is this path protected?
- How strong, or complex, is the algorithm used to encrypt and sign data?
- How are keys managed and distributed?
- Does the agency's use of cryptographic tools comply with related Federal Information Processing Standards issued by NIST?
- Has the entity chosen cryptographic techniques that are appropriate to cost-effectively meet its defined control objectives?

Exposure Draft

If the auditor encounters cryptographic tools and determines that their reliability is important to his or her understanding of the controls, they should obtain the most recent guidance available from OMB, NIST, and GAO, as well as technical assistance from an auditor experienced in assessing cryptographic tools.

Control Techniques and Suggested Audit Procedures for Critical Element AC-4

AC-4 Related NIST SP-800-53 Controls

AC-15 Automated Marking
AC-16 Automated Labeling
IA-7 Cryptographic Module Authentication
MP-2 Media Access
MP-3 Media Labeling
MP-4 Media Storage
MP-5 Media Transport
MP-6 Media Sanitization and Disposal
PE-19 Information Leakage
SC-2 Application Partitioning
SC-3 Security Function Isolation
SC-4 Information Remnance
SC-8 Transmission Integrity
SC-9 Transmission Confidentiality
SC-11 Trusted Path
SC-12 Cryptographic Key Establishment and Management
SC-13 Use of Cryptography
SC-16 Transmission of Security Parameters
SC-18 Mobile Code

Exposure Draft

Table 19. Control Techniques and Suggested Audit Procedures for Critical Element AC-4: Adequately protect sensitive system resources

Control activity	Control techniques	Audit procedures
AC-4.1. Access to sensitive system resources is restricted and monitored.	AC-4.1.1. Access to sensitive/privileged accounts is restricted to individuals or processes having a legitimate need for the purposes of accomplishing a valid business purpose.	Review pertinent policies and procedures. Interview management and systems personnel regarding access restrictions. Identify and test who has access to sensitive/privileged accounts and determine the reason for that access.
	AC-4.1.2. Use of sensitive/privileged accounts is adequately monitored.	Determine if the use of sensitive and privileged accounts is monitored and evaluate its effectiveness.
	AC-4.1.3. Logical access to utilities and tools is adequately controlled (for example, remote maintenance).	Determine the last time the access capabilities of system programmers were reviewed. Review security software settings to identify types of activity logged. Observe personnel accessing system software, such as sensitive utilities and note the controls encountered to gain access. Attempt to access the operating system and other system software. Select some application programmers and determine whether they are authorized access.
	AC-4.1.4. System libraries are appropriately controlled.	Determine if access to system libraries is adequately controlled.
	AC-4.1.5. Passwords/authentication services and directories are appropriately controlled and encrypted when appropriate.	Determine if password files and authentication services are adequately protected from unauthorized access.
	AC-4.1.6. Mobile code is appropriately controlled.	Interview system administrator and determine if mobile code is adequately controlled.
	AC-4.1.7. Where appropriate, access is restricted based on time and/or location.	Determine if access is appropriately restricted based on time and/or location.
	AC-4.1.8. The information system partitions or separates user functionality (including user interface services) from information system management functionality.	Interview officials and review related system documentation. Coordinate with vulnerability analysis.
	AC-4.1.9. The information system isolates security functions from nonsecurity functions.	Interview officials and review related system documentation. Coordinate with vulnerability analysis.
	AC-4.1.10. The information system establishes a trusted communications path between the user and the security functionality of the system.	Interview officials with system and communication responsibilities and examine appropriate records such as developer design documents.
AC-4.2. Adequate media controls have been implemented.	AC-4.2.1. Only authorized users have access to printed and digital media removed from the information system.	Interview personnel and review procedures. Observe entity practices and review selected access logs.

Exposure Draft

Control activity	Control techniques	Audit procedures
AC-4.3. Cryptographic controls are effectively used.	AC-4.2.2. The information system automatically identifies how information is to be used <ul style="list-style-type: none"> output is marked using standard naming conventions, and internal data in storage, process and transmission is labeled. 	Interview appropriate personnel. For output, identify standard naming conventions and examine the system configuration. For internal data, examine the labeling mechanism and internal data for accurate labels. Test output and internal data for appropriate results.
	AC-4.2.3. The organization controls the pickup, transport, and delivery of information system media (paper and electronic) to authorized personnel.	Interview officials and review appropriate policy and procedures. Observe selected media transport practices and receipts.
	AC-4.2.4. Systems media is securely stored according to its sensitivity.	Determine if media storage practices are adequate and comply with applicable requirements (for federal agencies, FIPS 199 security categories).
	AC-4.2.5. Security parameters are clearly associated with information exchanged between information systems.	Determine if security parameters are clearly associated with information exchanged.
	AC-4.2.6. Approved equipment, techniques, and procedures are implemented to clear sensitive data from digital media before its disposal or release for reuse outside of the organization.	Review written procedures; interview personnel responsible for clearing data from digital media. For a selection of recently discarded or transferred items, examine documentation related to clearing of data and disposal of software. For selected items still in the agency's possession, test to determine whether they have been appropriately sanitized.
	AC-4.3.1. Cryptographic tools have been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs.	Determine if cryptographic tools are properly implemented. (See NIST standards for federal agencies) To evaluate the use of cryptographic tools, the auditor should obtain the assistance of a specialist.
AC-4.3.2. Encryption procedures are implemented in data communications where appropriate based on risk.	Capture passwords transmitted over the network and determine if they are encrypted; for federal system, determine if cryptographic authentication complies with FIPS 140-2. To evaluate cryptographic tools, the auditor should obtain the assistance of a specialist.	
AC-4.3.3. For authentication to a cryptographic module, the information system employs appropriate authentication methods.	Interview appropriate officials and review supporting documentation. For federal agencies, compare the authentication process to FIPS 140-2 requirements.	
AC-4.3.4. The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.	Compare policy and practices to appropriate guidance, such as NIST guidance in SP 800-56 and SP 800-57 for cryptographic key establishment and management, respectively.	

Source: GAO.

Exposure Draft

Critical Element AC-5. Implement an effective audit and monitoring capability

Audit and monitoring involves the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the appropriate investigation and reporting of such activity. Automated mechanisms may be used to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. Audit and monitoring controls can help security professionals routinely assess computer security, perform investigations during and after an attack, and even recognize an ongoing attack. Audit and monitoring technologies include network and host-based intrusion detection systems, audit logging, security event correlation tools, and computer forensics. Network-based intrusion detection systems (IDSs) capture or “sniff” and analyze network traffic in various parts of a network. On the other hand, host-based IDSs analyze activity on a particular computer or host. Both types of IDS have advantages and disadvantages.

FISMA requires that each agency implement an information security program that includes procedures for detecting, reporting, and responding to security incidents. Further, OMB is to ensure the operation of a central federal information security incident center to

- provide timely technical assistance to system operators,
- compile and analyze incident information,
- inform system operators about threats and vulnerabilities, and
- consult with NIST, national security agencies, and other designated agencies such as the Department of Homeland Security.

NIST issued two relevant special publications that provide additional information:

- SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, and
- SP 800-61, *Computer Security Incident Handling Guide*

Exposure Draft

SP 800-61 discusses four steps in incident handling:

- preparation,
- detection and analysis,
- containment, eradication, and recovery, and
- post-incident activity.

An IDS detects inappropriate, incorrect, or anomalous activity aimed at disrupting the confidentiality, integrity, or availability of a protected network and its computer systems. An IDS collects information on a network, analyzes the information on the basis of a preconfigured rule set, and then responds to the analysis. A description of the technologies, their effectiveness, and how they work is described in *Technologies to Secure Federal Systems*, GAO-04-467 (Washington, D.C.: March 2004).

AC-5.1. An effective incident response program is documented and approved

An effective incident response program should be implemented. Control techniques include

- documented policies and procedures, including an incident response plan;
- documented testing of the incident response plan;
- a means of prompt centralized reporting;
- active monitoring of alerts and advisories;
- response team members with the necessary knowledge, skills, and abilities;
- training on roles and responsibilities and periodic refresher training;
- links to other relevant groups;
- protection against denial of service attacks; and
- appropriate incident response assistance and consideration of computer forensics.

OMB tasks NIST with coordinating activities governmentwide for agencies sharing information concerning common vulnerabilities and threats. Finally, Appendix III of OMB Circular A-130 directs the Department of Justice to provide appropriate guidance on pursuing legal remedies in the case of serious incidents.

Exposure Draft

According to NIST, the two main benefits of an incident-handling capability are (1) containing and repairing damage from incidents and (2) preventing future damage. Other, less obvious, benefits of an incident-handling capability include

- improved threat data for use in the risk assessment and control selection process,
- enhanced internal communication and organizational preparedness, and
- enhanced training and awareness programs by providing trainers with better information on users' knowledge and providing real-life illustrations for classes.

Also, according to NIST, the characteristics of a good incident-handling capability include

- an understanding of the constituency being served, including computer users and program managers;
- an educated constituency that trusts the incident-handling team;
- a means of prompt centralized reporting, such as through a hotline;
- a response team with the necessary knowledge, skills, and abilities, including technical expertise with the computer technology used by the agency, and the ability and willingness to respond when and where needed; and
- links to other groups—such as law enforcement agencies, response teams, or security groups external to the agency—and to the agency's public relations office (in case the incident receives media attention).

One aspect of incident response that can be especially problematic is gathering the evidence to pursue legal action. Incident response training and assistance is important for users of information systems to understand the proper handling and reporting of security incidents. Resources should be available to provide adequate computer forensics of security incidents. To gather evidence, an entity may need to allow an intruder or violator to continue his or her inappropriate activities—a situation that puts the system and

Exposure Draft

data at continued risk. However, fear of detection and prosecution can serve as a deterrent to future violations.

The United States Computer Emergency Readiness Team (US-CERT) was established in September 2003 to provide a national incident response capability. US-CERT is a partnership of the Department of Homeland Security and the public and private sectors. Established to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. Specifically, it is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

As the nation's focal point for preventing, protecting against, and responding to cyber security vulnerabilities, US-CERT interacts with all federal agencies, private industry, the research community, state and local governments, and others on a 24X7 basis to disseminate reasoned and actionable cyber security information. To provide security information to the public, US-CERT

- integrates content contributed by numerous organizations from both the public and private sectors,
- aggregates and analyzes the various types of data provided by contributing organizations,
- serves as the focal point for promoting common and comprehensive analysis of security trends and risks, and
- maintains quality control standards and works to ensure technical accuracy as well as timeliness.

Worldwide, there are more than 250 organizations that use the name CERT or a similar name and deal with cyber security response. US-CERT and the CERT Coordination Center at Carnegie Mellon University work jointly on cyber security activities. When a cyber security problem warrants, US-CERT coordinates a response by working with computer security experts from public and private state and local incident response teams. (See www.us-cert.gov/aboutus.html.)

Exposure Draft

In addition, the incident response program is affected by and should be responsive to the configuration of the entity's networks. For example, it can affect the placement of intrusion detection systems. Also, the network and related access controls can be designed to aid in containment of security breaches to limited areas of the network.

Also, the incident response program should appropriately consider treatment of privacy information. Specifically, federal entities should comply with applicable statutes and the following OMB Memoranda:

- M-06-15, *Safeguarding Personally Identifiable Information* (5/22/06)
- M-06-16, *Protection of Sensitive Agency Information* (6/23/06)
- M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (7/12/06)
- OMB Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (generally annual OMB memorandums)
- *Recommendations for Identity Theft Related Data Breach Notifications* (9/20/06)
- M-07-04, *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements* (12/22/06)

AC-5.2. Incidents are effectively identified and logged

Entity policies and procedures should establish criteria for the identification of significant system events that should be logged. Based on such criteria, the entity should identify significant system events. At a minimum, all such significant events,⁷⁰ including access

⁷⁰The checklists and configuration guides at <http://csrc.nist.gov/pcig/cig.html> provide recommended lists of auditable events.

Exposure Draft

to and modification of sensitive or critical system resources, should be logged. However, to be effective:

- this feature should be activated to log critical activity, maintain critical audit trails, and report unauthorized or unusual activity;
- access to audit logs should be adequately controlled; and
- managers should review logs for unusual or suspicious activity and take appropriate action.

Access control software should be used to maintain an audit trail of security access containing appropriate information for effective review to determine how, when, and by whom specific actions were taken. For example, time stamps of audit records should be generated using internal information system clocks that are synchronized systemwide. Such information is critical to monitoring compliance with security policies and when investigating security incidents. The settings of the access control software control the nature and extent of audit trail information provided. Typically, audit trails may include user ID, resource accessed, date, time, terminal location, and specific data modified. The information system should have the capability to determine whether or not a given individual took a particular action (non-repudiation).

The completeness and value of the audit trails maintained will only be as good as the agency's ability to thoroughly identify the critical processes and the related information that may be needed.

Procedures for maintaining such audit trails should be based on

- the value or sensitivity of data and other resources affected;
- the processing environment, for example, systems development, testing, or production;
- technical feasibility; and
- legal and regulatory requirements.

Audit trails, including automated logs, need to be retained for an appropriate period of time. Therefore, the entity needs to allocate sufficient audit record storage capacity and configure auditing to prevent the storage capacity from being exceeded. The information system should provide a warning when storage capacity reaches a

Exposure Draft

certain level. If storage capacity is reached, the system should alert appropriate officials and take appropriate, predefined actions such as saving the oldest data offline, shutting down the system, overwriting the oldest audit records, or stop generating audit records.

An effective intrusion detection system (IDS) should be implemented, including appropriate placement of intrusion-detection sensors and setting of incident thresholds. IDS security software generally provides a means of determining the source of a transaction or an attempted transaction and of monitoring users' activities (audit trail).

AC-5.3. Incidents are properly analyzed and appropriate actions taken

Because all of the audit trail and log information maintained is likely to be too voluminous to review on a routine basis, the IDS security software should be implemented to selectively identify unauthorized, unusual, and sensitive access activity, such as

- attempted unauthorized logical and physical access;
- access trends and deviations from those trends;
- access to sensitive data and resources;
- highly-sensitive privileged access, such as the ability to override security controls;
- access modifications made by security personnel; and
- unsuccessful attempts to logon to a system.

Modern information systems may have an audit-reduction and report-generation capability to automatically process audit records for events of interest based on selectable event criteria. The security software should be designed to report such activity and, in some cases, respond by actions such as

- disabling passwords,
- terminating repeated failed attempts to access sensitive resources,
- terminating processing,
- shutting down terminals,

Exposure Draft

- issuing warning or error messages, and
- writing audit trail records that would not normally be maintained.

Once unauthorized, unusual, or sensitive access activity is identified, it should be reviewed and apparent or suspected violations investigated. If it is determined that a security violation has occurred, appropriate action should be taken to identify and remedy the control weaknesses that allowed the violation to occur, repair any damage that has been done, and determine and discipline the perpetrator. It is important that an entity have formal written procedures for reporting security violations or suspected violations to a central security management office so that multiple related incidents can be identified, other employees can be alerted to potential threats, and appropriate investigations can be performed. Such incidents might include multiple attacks by a common hacker or repeated infections with the same computer virus.

Without prompt and appropriate responses to security incidents, violations could continue to occur and cause damage to an agency's resources indefinitely. Further, violators will not be deterred from continuing inappropriate access activity, which could cause embarrassment to the entity and result in disclosure of confidential information and financial losses.

An entity should have documented procedures in place for responding to security violations. These should include procedures and criteria for

- incident containment, eradication, and recovery
- documenting offenses,
- determining the seriousness of violations,
- reporting violations to higher levels of management,
- investigating violations,
- imposing disciplinary action for specific types of violations,
- notifying the resource owner of the violation,
- sharing incident and threat information with owners of connected systems, and

Exposure Draft

- reporting suspected criminal activity to law enforcement officials.

Further, access control policies and techniques should be modified when violations, incidents, and related risk assessments indicate that such changes are appropriate.

In addition, the frequency and magnitude of security violations and the corrective actions that have been taken should periodically be summarized and reported to senior management. Such a report can assist management in its overall management of risk by identifying the most attractive targets, trends in types of violations, cost of securing the agency's operations, and any need for additional controls.

Finally, since even the best incident response program may not catch increasingly sophisticated system intrusions, critical system resources should be periodically reviewed for integrity. For example, an organization may employ integrity verification applications on the information system to automatically look for evidence of information tampering, errors, and omissions.

<u>AC-5 Related NIST SP-800-53 Controls</u>

AC-13	Supervision and Review—Access Control
AT-5	Contacts with Security Groups and Associations
AU-2	Auditable Events
AU-3	Content of Audit Records
AU-4	Audit Storage Capacity
AU-5	Response to Audit Processing Failures
AU-6	Audit Monitoring, Analysis, and Reporting
AU-7	Audit Reduction and Report Generation
AU-8	Time Stamps
AU-9	Protection of Audit Information
AU-11	Audit Record Retention
IR-1	Incident Response Policy and Procedures
IR-2	Incident Response Training
IR-3	Incident Response Testing and Exercises
IR-4	Incident Handling
IR-5	Incident Monitoring
IR-6	Incident Reporting

Exposure Draft

IR-7	Incident Response Assistance
SC-5	Denial Of Service Protection
SI-4	Information System Monitoring Tools and Techniques
SI-6	Security Functionality Verification

Control Techniques and Suggested Audit Procedures for Critical Element AC-5

Table 20. Control Techniques and Suggested Audit Procedures for Critical Element AC-5: Implement an effective audit and monitoring capability

Control activity	Control techniques	Audit procedures
AC-5.1. An effective incident response program is documented and approved.	<p>AC-5.1.1. An effective incident-response program has been implemented and include</p> <ul style="list-style-type: none"> • documented policies, procedures, and plans; • documented testing of the incident response plan and follow-up on findings; • a means of prompt centralized reporting; • active monitoring of alerts/advisories; • response team members with the necessary knowledge, skills, and abilities; • training on roles and responsibilities and periodic refresher training; • links to other relevant groups; • protection against denial-of-service attacks (see http://icat.nist.gov); • appropriate incident-response assistance; and • consideration of computer forensics. 	<p>Interview security manager, response team members, and system users; review documentation supporting incident handling activities; compare practices to policies, procedures, and related guidance such as NIST SP 800-61 that provides guidance on incident-handling and reporting.</p> <p>Determine qualifications of response team members; review training records; identify training in incident response roles and responsibilities.</p> <p>Identify the extent to which computer forensics is used and compare to applicable guidelines and industry best practices.</p>
AC-5.2. Incidents are effectively identified and logged.	<p>AC-5.2.1. An effective intrusion detection system has been implemented, including appropriate placement of intrusion-detection sensors and incident thresholds.</p>	<p>Obtain the design and justification for the intrusion detection system; determine if the placement of sensors and incident thresholds is appropriate based on cost and risk.</p>
	<p>AC-5.2.2. An effective process has been established based on a risk assessment, to identify auditable events that will be logged.</p>	<p>Interview the security manager to determine the process for determining what actions are logged. Determine if security event correlation tools are used to identify anomalous network activity.</p>
	<p>AC-5.2.3. All auditable events, including access to and modifications of sensitive or critical system resources, are logged.</p>	<p>Review security software settings to identify types of activity logged; compare to NIST guidance on auditable events.</p>
	<p>AC-5.2.4. Audit records contain appropriate information for effective review including sufficient information to establish what events occurred, when the events occurred (for example, time stamps), the source of the events, and the outcome of the events.</p>	<p>Determine if audit records/logs are reviewed and whether they contain appropriate information; see appropriate NIST guidance.</p>
	<p>AC-5.2.5. Audit record storage capacity is adequate and configured to prevent such capacity from being exceeded. In the event of an audit failure or audit storage capacity being reached, the information system alerts officials and appropriate action is taken.</p>	<p>Determine the retention period for audit records and logs and whether it complies with applicable guidance. Determine if audit capacity is sufficient and what happens should it be exceeded.</p>

Exposure Draft

Control activity	Control techniques	Audit procedures
	AC-5.2.6. Audit records and tools are protected from unauthorized access, modification, and deletion. Audit records are effectively reviewed for unusual or suspicious activity or violations.	Determine how access to audit records/logs is controlled; review logs for suspicious activity and evidence of entity follow-up and appropriate corrective action.
	AC-5.2.7. Audit records are retained long enough to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Determine if audit record retention (for example, logs etc.) meet legal requirements and entity policy for computer forensics.
AC-5.3. Incidents are properly analyzed and appropriate actions taken.	AC-5.3.1. Security violations and activities, including failed logon attempts, other failed access attempts, and sensitive activity, are reported and investigated.	Review pertinent policies and procedures; review security violation reports; examine documentation showing reviews of questionable activities.
	AC-5.3.2. Security managers investigate security violations and suspicious activities and report results to appropriate supervisory and management personnel.	Test a selection of security violations to verify that follow-up investigations were performed and reported to appropriate supervisory and management personnel.
	AC-5.3.3. Appropriate disciplinary actions are taken.	For the sample in AC-5.3.2, determine what action was taken against the perpetrator.
	AC-5.3.4. Violations and incidents are analyzed, summarized, and reported to senior management and appropriate government authorities.	Interview senior management and personnel responsible for summarizing violations; review any supporting documentation. Determine if automated tools are used to analyze network activity and whether it complies with security policy.
	AC-5.3.5. Alerts and advisories are issued to personnel when appropriate.	Identify recent alerts and advisories and determine if they are up-to-date; interview entity personnel to determine what actions were taken.
	AC-5.3.6. Incident and threat information is shared with owners of connected systems.	Determine if incident and threat data are shared with owners of connected systems; follow up with owners of connected systems to see if they received this information in a timely manner.
	AC-5.3.7. Access control policies and techniques are modified when violations, incidents, and related risk assessments indicate that such changes are appropriate.	Review policies and procedures and interview appropriate personnel; review any supporting documentation.
	AC-5.3.8. Critical system resources are periodically reviewed for integrity.	Determine how frequently alterations to critical system files are monitored (for example, integrity checkers, etc.).
	AC-5.3.9. Appropriate processes are applied to gather forensic evidence in support of investigations.	Review entity processes to gather forensic information and determine whether they are adequate. Discuss with appropriate entity management.

Source: GAO.

Exposure Draft

Critical Element AC-6. Establish adequate physical security controls

Adequate physical security controls should be established that are commensurate with the risks of physical damage or access. In evaluating the effectiveness of physical security controls, the auditor should consider the effectiveness of the agency's policies and practices pertaining to both the overall facility and areas housing sensitive information technology components. Consequently, an entity should implement physical security controls in the following areas

- security planning and management (security management),
- securing the perimeter of the facility (perimeter security),
- controlling access into a facility (entry security),
- controlling access within a facility (interior security), and
- protection from emerging physical security threats (emerging threats).

Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. Computer resources to be protected include

- primary computer facilities,
- cooling system facilities,
- network devices such as routers and firewalls,
- terminals used to access a computer,
- microcomputers and mobile or portable systems,
- devices that display or output information,
- access to network connectivity, such as through "live" network jacks
- computer file storage areas, and
- telecommunications equipment and transmission lines.

In June 1995, the Department of Justice (DOJ) published minimum-security standards for the protection of federal facilities. It identified and evaluated the various types of security measures that could be used to counter potential vulnerabilities. The standards

Exposure Draft

cover perimeter security, entry security, interior security, and security planning. Because of the considerable differences among facilities and their security needs, physical holdings are divided into five security levels to determine which minimum standards are appropriate for which security levels.⁷¹ For federal agency facilities, appropriate criteria for physical safeguards in place for the overall facility are Justice standards unless the facility has adopted different standards. To illustrate, information technology resources may be housed in a facility that has been designated a national critical asset in accordance with Homeland Security Presidential Directive 7⁷² and therefore require physical security measures above those required by DOJ standards. For non-federal entities, appropriate criteria are equivalent guidance or the federal standards.

Physical controls also include environmental controls, such as smoke detectors, fire alarms, extinguishers, and uninterruptible power supplies (see section 3.5, service continuity).

In an IS controls audit being performed as part of a financial audit or data reliability assessment, the auditor should tailor the identification of control techniques and audit procedures related to the entity's physical security management program to the extent necessary to achieve the audit objectives, considering the IS controls identified by the auditor as significant to the audit objectives (e.g., internal control over financial reporting). Generally, this would include consideration of the overall design of the entity's physical security program at relevant facilities.

AC-6.1. Establish a physical security management program based on risk

Risk management is the foundation of an effective physical security program. The approach to good security is fundamentally similar,

⁷¹Department of Justice, *Vulnerability Assessment of Federal Facilities*, (Washington, D.C.: June 28, 1995).

⁷² *Critical Infrastructure Identification, Prioritization, and Protection* (Washington, D.C.: December 17, 2003).

Exposure Draft

regardless of the assets being protected—information systems, buildings, or critical infrastructure. Risk management principles for an effective security program are discussed in section 3.1. In addition, the testimonies *Technologies to Secure Federal Buildings* (GAO-02-687T) and *Key Elements of a Risk Management Approach* (GAO-02-150T) elaborate on specific risk management steps that may be applied to the protection of any critical asset.

The effectiveness of physical security controls depends on the effectiveness of the agency's policies and practices pertaining to the overall facility and to areas housing sensitive information technology components, including

- granting and discontinuing access authorizations,
- controlling badges, ID cards, smartcards, passkeys, and other entry devices,
- controlling entry during and after normal business hours,
- controlling the entry and removal of computer resources (for example, equipment and storage media) from the facility,
- managing emergencies,
- controlling reentry after emergencies,
- establishing compensatory controls when restricting physical access is not feasible, as is often the case with telecommunications lines, and
- storing computer assets such as equipment and sensitive documents.

In some instances an entity may not be able to fully control their physical security posture. For example, leased space in a building managed by another organization. In this case, the entity should consider compensating controls and ensure that contingency planning adequately considers their lack of control over physical security.

As with any type of business activity, physical security should be monitored to ensure that controls are accomplishing their intended purpose. FISMA specifically requires that federal agencies

Exposure Draft

periodically test and evaluate information security controls and techniques to ensure that they are effectively implemented.

Visitors should be controlled. On occasion, persons other than regularly authorized personnel may be granted access to sensitive areas or facilities, such as employees from another facility, maintenance personnel, contractors, and the infrequent or unexpected visitor. None of these visitors should be granted unrestricted access.⁷³ Controls should include

- preplanned appointments,
- identification checks,
- controlling the reception area,
- logging in visitors,
- escorting visitors while in sensitive areas, and
- periodically changing entry codes to prevent reentry by previous visitors who might have knowledge of the code.

AC-6.2. Establish adequate perimeter security based on risk

Perimeter security is the first line of defense against threats that can cause catastrophic damages to facilities and internal computer resources. Considerations for perimeter security include

- controlling vehicle and pedestrian traffic around the facility,
- controlling employee and visitor parking,
- monitoring the perimeter with closed circuit TV (CCTV),
- providing emergency backup power supply, and
- extending perimeter barriers to prevent unauthorized access and reduce exposure to explosions.

⁷³ Also see Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, (Washington, D.C.: August 27, 2004); and NIST Federal Information Processing Standard Publication (FIPS PUB) 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, (Washington, D.C.: March 2006).

Exposure Draft

Perimeter security includes protective controls such as fencing around sensitive buildings, concrete and earthen and other barriers, appropriate gates and locks, exterior lighting, guard posts, security patrols, and detection and monitoring systems.

AC-6.3. Establish adequate security at entrances and exits based on risk

Access to facilities should be limited to personnel having a legitimate need for access to perform their duties. Management should regularly review the list of persons authorized to have physical access to sensitive facilities, including contractors and other third parties. In addition, procedures should be implemented to terminate access privileges for terminated or separated employees or contractors.

Physical security controls at entrances and exits vary, but may include

- manual door or cipher key locks,
- magnetic door locks that require the use of electronic keycards,
- biometrics authentication,
- security guards,
- photo IDs,
- entry logs, and
- electronic and visual surveillance systems.

Unissued keys or other entry devices should be secure. Issued keys or other entry devices should be regularly inventoried.

AC-6.4. Establish adequate interior security based on risk

The effectiveness of physical security controls over sensitive and critical IT resources within a facility include consideration of whether the entity has

- identified all sensitive areas—such as individual rooms or equipment, software and tape libraries, or telecommunication closets and lines—that are susceptible to physical access, loss, or impairment;

Exposure Draft

- identified all physical access points and threats to the sensitive areas; and
- developed cost-effective security controls over all physical access points and addressed all significant threats to sensitive areas.

In addition, the entity should have controls to prevent or detect surreptitious entry into sensitive areas. For example, could unauthorized persons gain entry by

- observing lock combinations entered by authorized personnel?
- obtaining unsecured keycards?
- going over the top of a partition that stops at the underside of a suspended ceiling when the partition serves as a wall for a sensitive facility?
- cutting a hole in a plasterboard wall in a location hidden by furniture?

Many of the control techniques for interior security are similar to those for perimeter and entry security (for example, locks, surveillance systems, as well as using and controlling badges, ID cards, smartcards, passkey, and other entry devices). Additional considerations include

- logs and authorization for removal and return of tapes and other storage media to the library,
- computer terminal locks,
- controlled access to powerful consoles in data centers, and
- segregation of duties (discussed in section 3.4).

AC-6.5. Adequately protect against emerging threats based on risk

In addition to traditional physical security considerations, it may be important to protect building environments from new threats such as airborne chemical, biological, and radiological (CBR) attacks. Such protective measures may include the installation of early warning sensors, the location and securing of air intakes, and plans and procedures to mitigate the effect of a CBR release. The

Exposure Draft

decisions concerning which protective measures should be implemented for any building should be based on several factors, including the perceived risk associated with the building and its tenants, engineering and architectural feasibility, and cost.

Appropriate audit procedures related to emerging threats include:

- Interview appropriate officials to identify the level of physical security controls needed for the facility.
- Review the facility risk and independent assessments (for example, internal audit, internal office of physical security, outside consultants) to identify their assessment of risk and the adequacy of controls in place.
- Observe and document the controls in place. Assess the organization's preparations based on what the organization has stated it needs based on risk, including an evacuation plan for a possible CBR attack.
- Identify any planned projects to enhance physical security controls in this area through discussions with physical security and building management/operations staff.

Control Techniques and Suggested Audit Procedures for Critical Element AC-6

<u>AC-6 Related NIST SP-800-53 Controls</u>

PE-2 Physical Access Authorizations

PE-3 Physical Access Control

PE-4 Access Control for Transmission Medium

PE-5 Access Control Policy for Display Medium

PE-6 Monitoring Physical Access

PE-7 Visitor Control

PE-8 Access Records

Exposure Draft

Table 21. Control Techniques and Suggested Audit Procedures for Critical Element AC-6: Establish adequate physical security controls

Control activity	Control techniques	Audit procedures
AC-6.1. Establish an effective physical security management program based on risk.	AC-6.1.1. Use a risk management approach to identify the level of physical security needed for the facility and implement measures commensurate with the risks of physical damage or access.	Coordinate with sections SM-2 (assess and validate risks), SM-3 (policies and procedures), SD-1 (segregation of duties), and CP-2 (environmental controls). Interview entity officials to discuss how their physical security program is organized and whether they use a risk management approach. Obtain and review any facility risk assessments performed by the entity or by independent entities.
	AC-6.1.2. Facilities and areas housing sensitive and critical resources have been identified. The following generally constitute sensitive areas: computer rooms, tape libraries, telecommunication closets, mechanical/electrical rooms, cooling facilities and data transmission and power lines.	Review diagram of physical layout of the computer network, telecommunications, and cooling system facilities (for example, HVAC); inspect these areas for physical access control weaknesses.
	AC-6.1.3. All significant threats to the physical well-being of these resources have been identified and related risks determined.	Interview agency officials. Review risk analysis to ensure that it includes physical threats to employees and assets. Review any recent audit reports or other evaluations of the facility's physical security.
	AC-6.1.4. Establish law enforcement security liaisons that facilitate the accurate flow of timely security information between appropriate government agencies, provide procedures for the timely receipt and dissemination of threat information, and implement a standardized security/threat classifications and descriptions (for example, alert levels).	Check if the organization has established law enforcement security liaisons that facilitate the accurate flow of timely security information between appropriate government agencies. Review how the organization receives and disseminates security alerts. [Identify governmental agencies involved in the flow of security information and interview appropriate officials. Review procedures and nomenclature for threat information.]
	AC-6.1.5. Conduct annual employee physical security awareness training. Coordinate this step with SM-4.	Review information (for example, individual training records, training program content) on security awareness training and its frequency.
	AC-6.1.6. Security control procedures (for example, trusted vendors/suppliers, background checks, etc.) are established for non-employees (contractors, custodial personnel).	Review security control procedures for scope and adequacy.

Exposure Draft

Control activity	Control techniques	Audit procedures
	AC-6.1.7. Periodic monitoring and independent evaluations of the physical security program are conducted. Physical security incidents are effectively monitored and appropriate countermeasures are implemented. .	Check if the agency evaluates its physical security program and controls. Obtain and review the agency's most recent self assessments and compliance review report. Determine if security incidents are recorded, effectively analyzed, and result in appropriate countermeasures. Coordinate with SM-5: Monitor the effectiveness of the security program, and AC-5: Implement an effective audit and monitoring capability.
	AC-6.1.8. When possible, do not co-locate high risk operations with non-essential support organizations (for example, cafeteria, day care, banks, news media). If not possible, place appropriate security between such support organizations and critical facilities.	Identify co-located operations and their respective risk levels. Determine if the agency co-locates high risk operations with support operations and assess the security impact.
	AC-6.1.9. Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.	Review appointment and verification procedures for visitors, contractors, and maintenance personnel. Compare actual practices to procedures.
AC-6.2. Establish adequate perimeter security based on risk.	AC-6.2.1. Control/restrict vehicle and pedestrian traffic around the facility based on the facility's risk level. Specific measures include fences, gates, locks, guard posts, perimeter patrols and inspections.	Determine if vehicle and pedestrian traffic around the facility is adequately controlled for the risk level. Inspect the perimeter for physical security and access control weaknesses. Assess the effectiveness of perimeter guard procedures and practices for controlling access to facility grounds.
	AC-6.2.2. Control employee and visitor parking. For example, restrict access to facility parking and parking adjacent to the facility (including leases), use ID systems and procedures for authorized parking (for example, placard, decal, card key), have signs and arrangements for towing of unauthorized vehicles and adequate lighting for parking areas.	Observe parking area and related controls. Check if identification systems and procedures for authorized parking are in place. Determine what is done about unauthorized vehicles (e.g. towing).
	AC-6.2.3. Monitor the perimeter with closed circuit television (CCTV) including cameras with time lapse video recording and warning signs advising of 24 hour video surveillance.	Inspect the facility surveillance camera system to assess its capacity and ability to assist in protecting the facility's perimeter.
	AC-6.2.4. Lighting is adequate for effective surveillance and evacuation operations. Emergency power backup exists for lighting (as well as for alarm and monitoring systems).	Observe perimeter and exterior building lighting to determine its adequacy. Also, determine if emergency power is available for security systems. Request test results.
	AC-6.2.5. Extend perimeter barriers (for example, concrete, steel) and parking barriers, as needed, to prevent unauthorized access and reduce exposure to explosions.	Determine if perimeter barriers are used and extended if appropriate.
AC-6.3. Establish adequate security at entrances and exits based on risk.	AC-6.3.1. All employee access is authorized and credentials (for example, badges, identification cards, smart cards) are issued to allow access.	Observe and document all access control devices used to secure the facility.

Exposure Draft

Control activity	Control techniques	Audit procedures
	AC-6.3.2. Access is limited to those individuals who routinely need access through the use of guards, identification badges, or entry devices such as key cards.	Observe entries to and exits from facilities during and after normal business hours. Obtain a list of employees and contractors with badged access and check the justification for such access. Check whether terminated employees/contractors have turned in their badge.
	AC-6.3.3. Management conducts regular reviews of individuals with physical access to sensitive facilities to ensure such access is appropriate.	Review procedures used by management to ensure that individuals accessing sensitive facilities are adequately restricted. Evaluate support for physical access authorizations and determine appropriateness.
	AC-6.3.4. Intrusion detection systems with central monitoring capability are used to control access outside of normal working hours (for example, nights and weekends).	Determine if an intrusion detection system is used and test its use for appropriate exterior and interior apertures.
	AC-6.3.5. Visitor access logs are maintained and reviewed.	Compare entries in the log to a list of personnel authorized access.
	AC-6.3.6. X-ray and magnetometer equipment is used to screen people, possessions, and packages.	Observe how this equipment is used and test its effectiveness.
	AC-6.3.7. The entity controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items.	Review procedures and interview officials. Attempt to enter and exit the facility with information systems items at various entry points and times.
	AC-6.3.8. Entry and exit points are monitored by using CCTV capability. Also, high security locks and alarm systems are required for all doors that are not guarded.	Observe use of these devices and test as appropriate. Inspect the building(s) for physical access control weaknesses.
	AC-6.3.9. Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to reenter the facility after fire drills, etc.	Review written emergency procedures. Examine documentation supporting prior fire drills. Observe a fire drill.
AC-6.4. Establish adequate interior security based on risk.	AC-6.4.1. An ID badge should generally be displayed at <i>all</i> times. [All individuals must display an ID at all times.]	Observe use of employee and visitor IDs. See what happens if you do not display your own ID.
	AC-6.4.2. Visitors such as vendors, contractors, and service personnel who need access to sensitive areas are prescreened, formally signed in, badged and escorted.	Review visitor entry logs. Observe entries to and exits from sensitive areas during and after normal business hours. Interview guards at facility entry.
	AC-6.4.3. Sensitive information technology and infrastructure resources are adequately secured (for example, using keys, alarm systems, security software and other access control devices), including <ul style="list-style-type: none"> • the badging system, • computer room, master consoles, and tape libraries, • display and output devices, • data transmission lines, • power equipment and power cabling, • mobile or portable systems, and • utility and mechanical areas (HVAC, elevator, water). 	Interview officials. Walk through facilities and observe potential vulnerabilities and security controls [measures] used to protect sensitive information technology resources. Observe entries to and exits from sensitive areas during and after normal business hours. Review security software features and settings. Evaluate the badging system: who has access to the badging system and how it is protected; how is physical control is maintained over unissued and visitor badges. Test the controls.

Exposure Draft

Control activity	Control techniques	Audit procedures
	AC-6.4.4. Management conducts regular reviews of individuals with physical access to sensitive areas to ensure such access is appropriate.	Review procedures used by management to ensure that individuals accessing sensitive areas are adequately restricted. Determine if there is a periodic (e.g. annual) auditing and reconciliation of ID cards. Evaluate support for physical access authorizations and determine appropriateness.
	AC-6.4.5. As appropriate, physical access logs to sensitive areas are maintained and routinely reviewed.	Compare entries in the logs to a list of personnel authorized access.
	AC-6.4.6. Unissued keys, badges, or other entry devices are secured. Issued keys or other entry devices are regularly inventoried.	Observe practices for safeguarding keys, badges, and other devices.
	AC-6.4.7. Entry codes are changed periodically.	Review documentation of entry code changes.
	AC-6.4.8. All deposits and withdrawals of storage media from the library are authorized and logged.	Review procedures for the removal and return of storage media to and from the library. Select from the log some returns and withdrawals, verify the physical existence of the tape or other media, and determine whether proper authorization was obtained for the movement.
	AC-6.4.9. Documents/equipment are appropriately stored and are subject to maintenance and accountability procedures.	Examine and verify maintenance and accountability procedures for storage of documents and equipment.
	AC-6.4.10. Critical systems have emergency power supplies (for example, all alarm systems, monitoring devices, entry control systems, exit lighting, communication systems).	Verify that critical systems, (e.g., alarm systems, monitoring devices, entry control systems, exit lighting, and communication systems) have emergency power supplies. Identify back up systems and procedures and determine the frequency of testing. Review testing results.
AC-6.5. Adequately protect against emerging threats, based on risk	AC-6.5.1. Appropriate plans have been developed and controls implemented based on a risk assessment such as a shelter in place plan and/or evacuation plan for a potential CBR attack. [A plan is in place and tested to respond to emerging threats such as a CBR attack (e.g. an appropriate shelter in place and/or evacuation plan.)	Interview officials, review planning documents, and related test results. Observe and document the controls in place to mitigate emerging threats.
	AC-6.5.2. Outdoor areas such as air intakes, HVAC return air grilles, and roofs have been secured by restricting public access and relocating or protecting critical entry points (for example, air intake vents, protective grills, etc.)	Observe location of these devices and identify security measures that have been implemented.
	AC-6.5.3. All outdoor air intakes are monitored by CCTV, security lighting, and/or intrusion detection sensors.	Verify the existence of these controls.
	AC-6.5.4. The ventilation and air filtration system has been evaluated for vulnerabilities to CBR agents and remedial action taken based on cost and risks.	Interview officials and review the results of any evaluations.

Source: GAO.

Exposure Draft

3.3. Configuration Management (CM)

Configuration management (CM) involves the identification and management of security features for all hardware, software, and firmware components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. At an entitywide level, management develops security policies that establish the agency's configuration management process and may establish the configuration settings for the organization. Policy enforcement applications can be used to help administrators define and perform centralized monitoring and enforcement of an agency's security policies. These tools examine desktop and server configurations that define authorized access to specified devices and they compare these settings against a baseline policy. At a system level, network management provides system administrators with the ability to control and monitor a computer network from a central location. Network management systems obtain status data from network components, enable network managers to make configuration changes, and alert them of problems. For each critical control point, at each system sublevel (for example, network, operating systems, and infrastructure applications), the entity should have configuration management controls to ensure that only authorized changes are made to such critical components. At a business process application level, all applications and changes to those applications should go through a formal, documented systems development process that identifies all changes to the baseline configuration. Also, procedures should ensure that no unauthorized software is installed.

In some instances, the entity may not have an effective entitywide configuration management process, but may nonetheless have configuration management controls at the systems and business process application level. Therefore, evaluation of configuration controls at all levels is important to determine whether they are effective.

FISMA requires each federal agency to determine minimally acceptable system configuration requirements and ensure compliance with them. Systems with secure configurations have less

Exposure Draft

vulnerability and are better able to thwart network attacks. In response to both FISMA and the Cyber Security Research and Development Act, NIST developed a central repository for information technology security configuration checklists: <http://checklists.nist.gov>. Typically, checklists are created by information technology vendors for their own products; however, checklists are also created by other entities such as consortia, academia, and government agencies. Security configuration checklists are a series of instructions for configuring a product to a particular operational environment. Some examples of the types of devices and software for which security checklists are intended are as follows:

- general purpose operating systems
- common desktop applications such as e-mail clients, Web browsers, word processing, personal firewalls, and antivirus software
- infrastructure devices such as routers, firewalls, virtual private network (VPN) gateways, intrusion detection systems (IDS), wireless access points (WAP), and telecom systems
- application servers such as domain name system (DNS) servers, dynamic host configuration protocol (DHCP) servers, Web servers, simple mail transfer protocol (SMTP) servers, file transfer protocol (FTP) servers, and database servers
- other network devices such as mobile devices, scanners, printers, copiers, and fax appliances

Industry best practices, NIST, and DOD guidance⁷⁴ all recognize the importance of configuration management when developing and maintaining a system or network. Through configuration management, the composition of a system is formally defined and tracked to ensure that an unauthorized change is not introduced. Changes to an information system can have a significant impact on the security of the system. Documenting information system changes and assessing the potential impact on the security of the

⁷⁴See, for example, IEEE Standard 1200-1998, SEI CMMI (ver. 1.1), NIST SP 800-64, and Military Handbook 61A(SE).

Exposure Draft

system on an ongoing basis is an essential aspect of maintaining the security posture. An effective entity configuration management and control policy and associated procedures are essential to ensuring adequate consideration of the potential security impact of specific changes to an information system. Configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the entity and subsequently controlling and maintaining an accurate inventory of any changes to the system.

An effective configuration management process consists of four primary concepts, each of which should be described in a configuration management plan and implemented according to the plan. The four are:

- *configuration identification*: procedures for identifying, documenting, and assigning unique identifiers (for example, serial number and name) to a system's hardware and software component parts and subparts, generally referred to as configuration items
- *configuration control*: procedures for evaluating and deciding whether to approve changes to a system's baseline configuration; decision makers such as a configuration control board evaluate proposed changes on the basis of costs, benefits, and risks, and decide whether to permit a change
- *configuration status accounting*: procedures for documenting and reporting on the status of configuration items as a system evolves. Documentation, such as historical change lists and original designs or drawings, are generated and kept in a library, thereby allowing entities to continuously know the state of a system's configuration and be in a position to make informed decisions about changing the configuration.
- *configuration auditing*: procedures for determining alignment between the actual system and the documentation describing it, thereby ensuring that the documentation used to support decision making is complete and correct. Configuration audits are performed when a significant system change is introduced and help to ensure that only authorized changes are being made and that systems are operating securely and as intended.

Exposure Draft

Establishing controls over the modification of information system components and related documentation helps to ensure that only authorized systems and related program modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all hardware, software, and firmware programs and program modifications are properly authorized, tested, and approved, and that access to and distribution of computer assets is carefully controlled. Without proper controls, there is a risk that security features could be inadvertently or deliberately omitted or turned off or that processing irregularities or malicious code could be introduced. For example,

- a knowledgeable programmer could modify program code to provide a means of bypassing controls to gain access to sensitive data;
- the wrong version of a program could be implemented, thereby perpetuating outdated or erroneous processing that is assumed to have been updated; or
- a virus could be introduced, inadvertently or on purpose, that disrupts processing.

Effective configuration management prevents unauthorized changes to information system resources (for example, software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended.

The absence of effective system-level configuration management is a serious risk that jeopardizes an agency's ability to support current and potential requirements. Without effective configuration management, users do not have adequate assurance that the system and network will perform as intended and to the extent needed to support their missions.

Assessing controls over configuration management involves evaluating the agency's success in performing each of the critical elements listed in table 22. Also, NIST SP 800-100 provides guidance in related configuration management programmatic areas of capital planning and investment control, and security services and product acquisition. This publication discusses practices designed to help security managers identify funding needs to secure systems and

Exposure Draft

provide strategies for obtaining the necessary funding. In addition, it provides guidance to entities in applying risk management principles to assist in the identification and mitigation of risks associated with security services acquisitions.

Table 22. Critical Elements for Configuration Management

Number	Description
CM-1.	Develop and document CM policies, plans, and procedures
CM-2.	Maintain current configuration identification information
CM-3.	Properly authorize, test, approve, and track all configuration changes
CM-4.	Routinely monitor the configuration
CM-5.	Update software on a timely basis to protect against known vulnerabilities
CM-6.	Appropriately document and approve emergency changes to the configuration

Source: GAO

Critical Element CM-1. Develop and document CM policies, plans, and procedures

Configuration management policies, plans, and procedures should be developed, documented, and implemented at the entitywide, system, and application levels to ensure an effective configuration management process. Such procedures should cover employee roles and responsibilities, change control and system documentation requirements, establishment of a decision-making structure, and configuration management training. CM should be a key part of an agency's Systems Development Life Cycle (SDLC) methodology.⁷⁵

An effective entitywide SDLC methodology details the procedures that are to be followed when systems and applications are being designed and developed, as well as when they are subsequently modified. The SDLC should provide a structured approach for identifying and documenting needed changes to computerized operations; assessing the costs and benefits of various options, including the feasibility of using off-the-shelf software; and designing, developing, testing, and approving new systems and system modifications. It is especially important that, for new

⁷⁵A Systems Development Life Cycle (SDLC) methodology consists of the policies and procedures that govern software development and modification as a software product goes through each phase of its life cycle.

Exposure Draft

systems being developed or for major enhancements to existing systems, SDLC require approving design features at key points during the design and development process. For the methodology to be properly applied, it should be sufficiently documented to provide staff with clear and consistent guidance. Also, personnel involved in designing, developing, and implementing new systems and system modifications should be appropriately trained. This includes program staff who initiate requests for modifications and staff involved in designing, programming, testing, and approving changes. NIST SP 800-64, dated October 2003, identifies security considerations in the information system development life cycle. In addition, NIST SP 800-27 provides guidance on engineering principles for designing security into information systems.

Configuration management policies and procedures should describe the configuration management process and address purpose, scope, roles, responsibilities, compliance, and implementation of security controls. Security controls include the following.

- A baseline configuration of the information system and an inventory of the system's constituent components.
- A process to document and control changes to the system.
- Monitoring system changes and analysis of their impact to determine the effect of the changes.
- Access restrictions over changes to the system and auditing of the enforcement actions.
- Configuring the security settings of information technology products to the most restrictive mode consistent with operational requirements.
- Configuring the information system to provide only essential capabilities and specifically prohibiting or restricting the use of unnecessary or dangerous functions, ports, protocols, and services.

Good configuration management provides strict control over the implementation of system changes and thus minimizes corruption to information systems.

Exposure Draft

Also, CM policies should address the introduction of software developed outside of the entity's normal software development process, including commercial or other software acquired by individual users.

Configuration management plans should address configuration management in terms of the following:⁷⁶

- responsibilities and authorities for accomplishing the planned activities (who)
- activities to be performed (what)
- required coordination of configuration management activities with other activities (when)
- tools and physical and human resources required for the execution of the plan as well as how the plan will be kept current (how)

The CM plan should describe the allocation of responsibilities and authorities for CM activities to entities and individuals within the project structure. Organizational units may consist of a vendor and customer, a prime contractor and subcontractors, or different groups within one entity. The name of the organizational unit or job title to perform this activity is provided for each activity listed within CM activities. A matrix that relates these entities to CM functions, activities, and tasks is useful for documenting CM activities. CM activities identify all functions and tasks required to manage the configuration as specified in the scope of the CM plan. CM activities are traditionally grouped into four functions: configuration identification, configuration control, configuration status accounting, and configuration audits and reviews.

Configuration management procedures should describe the configuration management system used to maintain and change

⁷⁶Based on IEEE Standard for Software Configuration Management Plans (IEEE Std. 828-1998), the Institute of Electrical and Electronic Engineers, June 25, 1998.

Exposure Draft

controlled work products. A configuration management system includes the storage media, the procedures, and the tools for accessing the configuration system. The procedures should describe how configuration items are stored and retrieved; shared between control levels; recovered; protected by access controls; and stored, updated, and retrieved. Configuration management plans should be integrated at all levels.

CM-1 Related NIST SP-800-53 Controls
 CM-1 Configuration Management Policy and Procedures

Control Techniques and Suggested Audit Procedures for Critical Element CM-1

Table 23. Control Techniques and Suggested Audit Procedures for Critical Element CM-1: Develop and document CM policies, plans, and procedures

Control activities	Control techniques	Audit procedures
CM-1.1. CM policies, plans and procedures have been developed, documented, and implemented.	CM-1.1.1. An effective configuration management process is documented and implemented, including: <ul style="list-style-type: none"> • a CM plan that identifies roles, responsibilities, procedures, and documentation requirements; • guidance that is appropriate for personnel with varying levels of skill and experience; • trained personnel who are familiar with the organization's configuration management process; • permitting only essential capabilities and restricting the use of dangerous functions, ports, protocols, and services; • regular review and approval of configuration changes by management (for example, Configuration Control Board); • a formal SDLC methodology that includes system-level security engineering principles to be considered in the design, development, and operation of an information system. • appropriate systems documentation. 	Review CM policies, plans, and procedures to identify roles, responsibilities, procedures, and documentation requirements. Determine if a CCB exists and is operating effectively. Interview staff and review training records. Interview hardware and software managers to identify the currency and completeness of CM policies, plans, procedures, and documentation. Review CM documentation and test whether recent changes are incorporated. Review the SDLC methodology and ensure that security is adequately considered throughout the life cycle. Review a selection of system documentation to verify that the SDLC methodology was followed and complies with appropriate guidance, such as NIST SP 800-64 and SP 800-27.

Source: GAO.

Critical Element CM-2. Maintain current configuration identification information

Configuration identification activities involve identifying, naming, and describing the physical and functional characteristics of a controlled item (for example, specifications, design, IP address,

Exposure Draft

code, data element, architectural artifacts, and documents). The CM plan should describe how each configuration item and its versions are uniquely named. It should also describe the activities performed to define, track, store, manage, and retrieve configuration items. Configuration items should be associated with development and production baselines.

The entity should maintain current configuration information in a formal configuration baseline that contains the configuration information formally designated at a specific time during a product's or product component's life. Configuration baselines, plus approved changes from those baselines, constitute the current configuration information. There should be a current and comprehensive baseline inventory of hardware, software, and firmware, and it should be routinely validated for accuracy. Backup copies of the inventory should be maintained and adequately protected. There should also be information system diagrams and documentation on the set up of routers, switches, guards, firewalls, and any other devices facilitating connections to other systems. FISMA requires federal agency compliance with system configuration guidelines, as determined by the agency. In addition, OMB Memorandum M-07-11⁷⁷ requires agencies that upgrade to the Microsoft Vista[™] operating system to adopt the security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DoD) and the Department of Homeland Security (DHS).

<u>CM-2 Related NIST SP-800-53 Controls</u>

CM-2 Baseline Configuration

CM-6 Configuration Settings

CM-8 Information System Component Inventory

SA-5 Information System Documentation

⁷⁷ OMB, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems (Washington, D.C.: March 22, 2007).

Exposure Draft

Control Techniques and Suggested Audit Procedures for Critical Element CM-2

Table 24. Control Techniques and Suggested Audit Procedures for Critical Element CM-2: Maintain current configuration identification information

Control activities	Control techniques	Audit procedures
CM-2.1. Current configuration identification information is maintained.	CM-2.1.1. A current and comprehensive baseline inventory of hardware, software, and firmware is documented, backed up, and protected. Information system documentation describes security controls in sufficient detail to permit analysis and testing of controls.	Request an inventory of all computer assets and determine if the inventory is accurate, complete, and whether duplicate copies are adequately protected. Sample items in the inventory and trace to the asset and verify that the configuration (model, settings, etc.) is accurate. Sample assets at the entity and verify that they are accurately recorded in the inventory.
	CM-2.1.2. Configuration settings optimize the system's security features.	Determine if key component security settings conform with NIST SP 800-70 and vendor recommendations.

Source: GAO.

Critical Element CM-3. Properly authorize, test, approve, track, and control all configuration changes

An entity should properly control all configuration changes; not only changes made by internal developers but also changes made by external developers or contractors (see SM-7 for activities performed by external third parties). This includes a wide range of activities starting with the establishment of a formal change management process. Management should authorize and approve all configuration changes. Test plan standards should be developed for all levels of testing and test plans should be documented and approved by all responsible parties. Testing should be comprehensive and appropriately consider security and impacts on interfacing systems. An audit trail should be made to clearly document and track the configuration changes.

Authorizations for system and application software modifications should be documented and maintained. Policies and procedures should be in place that detail who can authorize a modification and how these authorizations are to be documented. Generally, the application users have the primary responsibility for authorizing system changes; however, users should be required to discuss their proposed changes with systems developers to confirm that the change is feasible and cost effective. For this reason, an entity may require a senior systems developer to co-authorize a change. The

Exposure Draft

use of standardized change request forms helps ensure that requests are clearly communicated and that approvals are documented. Authorization documentation should be maintained for at least as long as a system is in operation in case questions arise regarding why or when system modifications were made. Authorization documents may be maintained in either paper or electronic form as long as their integrity is protected.

Configuration control activities involve activities that request, evaluate, approve, disapprove, or implement changes to baseline configuration items. Changes encompass both error correction and enhancements. The configuration management plan should identify each level of decision making (for example, CCB⁷⁸) and its level of authority for approving proposed system and application changes and its management of development and production baselines.

The configuration status accounting process records and reports the status of configuration items. The following are minimum data elements to be tracked for a configuration item: (1) its initial approved version, (2) the status of requested changes, and (3) the implementation status of approved changes. The level of detail and specific data required may vary according to the information needs of the project and the customer.

A disciplined process for testing and approving new and modified systems before their implementation is essential to make sure systems hardware and related programs operate as intended and that no unauthorized changes are introduced. Test plans should appropriately consider security. The extent of testing varies depending on the type of modification. For new systems being developed or major system enhancements, testing will be extensive, generally progressing through a series of test stages that include (1) testing individual program modules (unit testing), (2) testing groups of modules that must work together (integration testing), and (3) testing an entire system (system testing). Minor modifications may require less extensive testing; however, changes

⁷⁸A configuration control board evaluates and approves or disapproves proposed changes to configuration items and ensures implementation of approved changes.

Exposure Draft

should still be carefully controlled and approved since relatively minor program code changes, if performed incorrectly, can have a significant impact on security and overall data reliability.

Once a change has been authorized, it should be implemented, written into the program code, and tested in a disciplined manner. Because testing is an iterative process that is generally performed at several levels, it is important that the entity adhere to a formal set of configuration management procedures or standards for prioritizing, scheduling, testing, and approving changes. These procedures

should be described in the agency's configuration management plan and should include requirements for

- ranking and scheduling configuration changes so that authorized change requests are not lost and are implemented efficiently and in accordance with user needs;
- preparing detailed specifications for the configuration change, which are approved by an individual responsible for supervising programming activities to confirm that the specifications correspond to the user's authorized requirements;
- developing a detailed test plan for each modification that defines the levels and types of tests to be performed;
- defining responsibilities for each person involved in testing and approving software (for example, systems analysts, programmers, quality assurance staff, auditors, library control personnel, and users—who should participate in testing and approve test results before implementation), including determining that testing is performed by parties independent of development;
- developing related configuration changes to system documentation, including hardware documentation, operating procedures, and user procedures;
- supervisory review and documented approvals by appropriate personnel, including programming supervisors, database administrators, and other technical personnel before and after testing;
- maintaining controlled libraries of software in different stages of development to ensure that programs being developed or tested

Exposure Draft

are not interchanged with each other or with production software;

- documenting configuration/software changes so that they can be traced from authorization to the final approved code and facilitating “trace-back” of code to design specifications and functional requirements by system testers; and
- obtaining final user acceptance only after testing is successfully completed and reviewed by the user.

To ensure that approved software programs are protected from unauthorized changes or impairment and that different versions are not misidentified, copies should be maintained in carefully controlled libraries. Further, adequately controlled software libraries help ensure that there is (1) a copy of the official approved version of a program available in case the integrity of an installed version is called into question and (2) a permanent historical record of old program versions.

Separate libraries should be established for programs being developed or modified, programs being tested by users, and programs approved for use (production programs). Access to these libraries should be limited and movement of programs and data among them should be controlled.

Inadequately controlled software libraries increase the risk that unauthorized changes could be made either inadvertently or deliberately for fraudulent or malicious purposes. In addition, inadequate controls over programs being developed or modified could make it difficult to determine which version of the program is the most recent. Such an environment can result in inefficiencies and could lead to interruptions of service and monetary losses. For example,

- an unauthorized program could be substituted for the authorized version;
- test programs could be labeled as production programs;
- two programmers could inadvertently access and work on the same test program version simultaneously, making it difficult or impossible to merge their work; or

Exposure Draft

- unauthorized changes to either test or production programs could be made and remain undetected.

Copies of software programs should be maintained in libraries where they are labeled, dated, inventoried, and organized in a way that diminishes the risk that programs will be misidentified or lost. Library management software provides an automated means of inventorying software (ensuring that differing versions are not accidentally misidentified) and maintaining a record of software changes. Specifically, such software can be used to

- produce audit trails of program changes and maintain version number control,
- record and report program changes made,
- automatically number program versions,
- identify creation date information,
- maintain copies of previous versions, and
- control concurrent updates so that multiple programmers are prevented from making changes to the same program in an uncontrolled manner.

The movement of programs and data among libraries should be controlled by an entity group or person that is independent of both the user and the programming staff. This group should be responsible for

- moving programs from development/maintenance to user testing and from user testing to production;
- supplying data from the production library for testing and creating test data; and
- controlling different program versions, especially when more than one change is being performed on a program concurrently.

Before transferring a tested program from the user test library to the production library, the independent library control group should (1) generate a report that shows all changed source code (lines added, changed, and deleted) and (2) compare this report to the user request to ensure that only approved changes were made.

Exposure Draft

Many federal agencies have data processing operations that involve multiple locations and require a coordinated effort for effective and controlled distribution and implementation of new or revised software. For example, an entity may have a central software design, development, and maintenance activity, but have two or more regional data processing centers running the same software. Once a modified software program has been approved for use, the change should be communicated to all affected parties and distributed and implemented in a way that leaves no doubt about when it is to begin affecting processing. To accomplish these objectives, an entity should have and follow established procedures for announcing approved changes and their implementation dates and for making the revised software available to those who need to begin using it.

Source code programs (the code created by programmers) are compiled into object or production code programs that are machine-readable and become the versions that are actually used during data processing. Source code programs should be closely controlled at a central location and compiled into production programs before being distributed. Source code should not be distributed to other locations. This helps protect the source code from unauthorized changes and increases the integrity of the object or production code, which is much more difficult for programmers to change without access to the source code. Inadequately controlling software distribution and implementation increases the risk that data could be improperly processed due to

- implementation of unapproved and possibly malicious software,
- continued use of outdated versions of software, and
- inconsistent implementation dates resulting in inconsistent processing of similar data at different locations.

With independent processing sites, each site is responsible for implementing the correct version of the software at the predetermined date and time and maintaining the documentation authorizing such implementation. Conversely, implementing new software through one or more central computers or servers

Exposure Draft

minimizes the risk that the software will be inconsistently implemented.

The use of public domain and personal software should be restricted. It is important that an entity have clear policies regarding the use of personal and public domain software by employees at work. Allowing employees to use their own software or even diskettes for data storage that have been used elsewhere increases the risk of introducing viruses. It also increases the risk of violating copyright laws and making bad decisions based on incorrect information produced by erroneous software. As mentioned in section CM-5, virus identification software can help contain damage from viruses that may be introduced from unauthorized use of public domain, from personal software, or from corrupted diskettes.

<p><u>CM-3 Related NIST SP-800-53 Controls</u> CM-3 Configuration Change Control SA-2 Allocation of Resources SA-3 Life Cycle Support SA-4 Acquisitions SA-8 Security Engineering Principles SA-10 Developer Configuration Management SA-11 Developer Security Testing</p>
--

Control Techniques and Suggested Audit Procedures for Critical Element CM-3

Table 25. Control Techniques and Suggested Audit Procedures for Critical Element CM-3: Properly authorize, test, approve, and track all configuration changes

Control activities	Control techniques	Audit procedures
CM-3.1. All configuration changes are properly managed (authorized, tested, approved, and tracked).		Where appropriate, these audit procedures should be applied to both internal and external developers and coordinated with section SM-7. (Ensure that activities performed by external third parties are adequately secure.)
	CM-3.1.1. An appropriate formal change management process is documented.	Review the change management methodology for appropriateness. Review system documentation to verify that the change management methodology was followed.

Exposure Draft

CM-3.1.2. Configuration changes are authorized by management. Configuration management actions are recorded in sufficient detail so that the content and status of each configuration item is known and previous versions can be recovered.	Examine a selection of CM and software change request forms for approvals and sufficiency of detail. Interview CM management and software development staff.
CM-3.1.3. Relevant stakeholders have access to and knowledge of the configuration status of the configuration items.	Interview users and ensure that they have ready access to software change requests, test reports, and configuration items associated with the various baselines being managed.
CM-3.1.4. Detailed specifications are prepared by the programmer and reviewed by a programming supervisor for system and application software changes.	For the software change requests selected for control activity CM-3.1.2: <ul style="list-style-type: none">• review specifications and related documentation for evidence of supervisory review.
CM-3.1.5. Test plan standards have been developed for all levels of testing that define responsibilities for each party (for example, users, system analysts, programmers, auditors, quality assurance, library control).	Review test plan standards.
CM-3.1.6. Test plans are documented and approved that define responsibilities for each party involved (for example, users, systems analysts, programmers, auditors, quality assurance, library control).	For the software change requests selected for control activity CM-3.1.2: <ul style="list-style-type: none">• review test plans;• compare test documentation with related test plans;• analyze test failures to determine if they indicate ineffective software testing;• review test transactions and data;• review test results;• review documentation for appropriate supervisory or management reviews;• verify user acceptance; and• review updated documentation.
CM-3.1.7. Test plans include appropriate consideration of security.	Determine whether operational systems experience a high number of system failures (for example, bends) and, if so, whether they indicate inadequate testing before implementation.
CM-3.1.8. Unit, integration, and system testing are performed and approved in accordance with the test plan and apply a sufficient range of valid and invalid conditions.	Examine a selection of program changes to determine whether they were approved by management prior to being moved to production.
CM-3.1.9. A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing.	Examine procedures for distributing new software.
CM-3.1.10. Live data are not used in testing of program changes, except to build test data files.	
CM-3.1.11. Test results are documented and appropriate responsive actions are taken based on the results.	
CM-3.1.12. Program changes are moved into production only when approved by management and by persons independent of the programmer.	
CM-3.1.13. Standardized procedures are used to distribute new software for implementation.	

Exposure Draft

<p>CM-3.1.14. Appropriate tools (for example, library mgt. software and manual techniques) are used to:</p> <ul style="list-style-type: none">• produce audit trails of program changes,• maintain program version numbers,• record and report program changes,• maintain creation/date information for production modules,• maintain copies of previous versions, and• control concurrent updates.	<p>Review pertinent policies and procedures. Interview personnel responsible for appropriate tools and library control. Examine a selection of programs maintained in the library and assess compliance with prescribed procedures. Determine whether documentation is maintained on program changes, program version numbers, creation/date information, and copies of prior versions. Review procedures for controlling concurrent updates.</p>
<p>CM-3.1.15. Configuration/software changes are documented so that they can be traced from authorization to the final approved code and they facilitate “trace-back” of code to design specifications and functional requirements by system testers.</p>	<p>For the software change requests selected for control activity CM-3.1.2:</p> <ul style="list-style-type: none">• trace changes from authorization to the final approved code; and,• trace changes back from code to design specifications and functional requirements.
<p>CM-3.1.16. Program development and maintenance, testing, and production programs are maintained separately (for example, libraries) and movement between these areas is appropriately controlled, including appropriate consideration of segregation of duties (see the Segregation of Duties control area.</p>	<p>Review pertinent policies and procedures and interview library control personnel. Examine libraries in use. Test access to program libraries by examining security system parameters.</p> <p>Review program changes procedures for adherence to appropriate segregation of duties between application programming and movement of programs into production.</p> <p>For a selection of program changes, examine related documentation to verify that (1) procedures for authorizing movement among libraries were followed and (2) before and after images were compared.</p>
<p>CM-3.1.17. Access to all programs, including production code, source code, and extra program copies, are adequately protected.</p>	<p>For critical software production programs, determine whether access control software rules are clearly defined. Test access to program libraries by examining security system parameters.</p>
<p>CM-3.1.18. Configuration changes to network devices (for example, routers and firewalls) are properly controlled and documented.</p>	<p>Review a sample of configuration settings to key devices and determine if configuration changes are adequately controlled and documented.</p>
<p>CM-3.1.19. Clear policies restricting the use of personal and public domain software and prohibiting violations of software licensing agreements have been developed and are enforced.</p>	<p>Review pertinent policies and procedures. Interview users and data processing staff. Review and test management enforcement process.</p>

Source: GAO.

Exposure Draft

Critical Element CM-4. Routinely monitor the configuration

Current configuration information should be routinely monitored for accuracy. Monitoring should address the current baseline and operational configuration of the hardware, software, and firmware that comprise the information system. Information technology products should comply with applicable standards and the vendors' good security practices. The entity should have the capability to monitor and test that it is functioning as intended. Also, networks should be appropriately configured and monitored to adequately protect access paths between information systems.

Monitoring, sometimes called configuration audits, should be periodically conducted to determine the extent to which the actual configuration item reflects the required physical and functional characteristics originally specified by requirements. The configuration plan should identify the frequency of configuration audits. A configuration audit should be performed on a configuration item before its release and it should be routinely tested thereafter. Configuration audits establish that the functional and performance requirements defined in the configuration documentation have been achieved by the design and that the design has been accurately documented in the configuration document. The purpose and benefits of the process include the following:

- Ensures that the product design provides the agreed-to performance capabilities
- Validates the integrity of the configuration documentation
- Verifies the consistency between a product and its configuration documentation
- Determines that an adequate process is in place to provide continuing control of the configuration
- Provides confidence in establishing a product baseline
- Ensures a known configuration as the basis for operation and maintenance instructions, and training.

Security settings for network devices, operating systems, and infrastructure applications need to be monitored periodically to

Exposure Draft

ensure that they have not been altered and that they are set in the most restrictive mode consistent with the information system operational requirements. NIST SP 800-70 provides guidance on configuration settings (for example, checklists) for information technology products.

A process and related procedures needs to be established to document the results from monitoring configuration items and ensure that discrepancies are properly corrected. For example, network and host environments should be scanned on a regular basis to determine whether patches have been effectively applied. A formal process with central management helps to ensure patch compliance with the network configuration. Audit results need to be recorded indicating

- each discrete requirement,
- method of verification,
- verification procedures,
- verification results, and
- corrective actions.

<p>CM-4 <u>Related NIST SP-800-53 Controls</u> CM-4 Monitoring Configuration Changes CM-5 Access Restrictions for Change SI-7 Software and Information Integrity</p>
--

Exposure Draft

Control Techniques and Suggested Audit Procedures for Critical Element CM-4

Table 26. Control Techniques and Suggested Audit Procedures for Critical Element CM-4: Routinely monitor the configuration

Control activities	Control techniques	Audit procedures
CM-4.1. The configuration is routinely audited and verified.	CM-4.1.1. Routinely validate that the current configuration information is accurate, up-to-date, and working as intended for networks, operating systems, and infrastructure applications.	Identify the standards and procedures used to audit and verify the system configuration. Determine when and how often the configuration is verified and audited. Review a sample of the configuration verifications and audits for compliance with applicable standards. Verify that vendor-supplied system software is still supported by the vendor. Evaluate adequacy of the configuration audits based on the results of the IS control audit tests performed.
	CM-4.1.2. The verification and validation criteria for the configuration audit is appropriate and specifies how the configuration item will be evaluated in terms of correctness, consistency, necessity, completeness, and performance.	Review evaluation criteria for the release. Identify all configuration items, deviations and waivers, and the status of tests. Determine if configuration items have gaps in the documentation or if there are defects in the change management process.
	CM-4.1.3. Confirm compliance with applicable configuration management policy, plans, standards, and procedures.	Compare configuration policy, plans, standards, and procedures with observations.
	CM-4.1.4. The information system periodically verifies the correct operation of security functions—on system start up and restart, on command by user with appropriate privilege—(providing system audit trail documentation) and takes appropriate action (for example, notifies system administrator, shuts the system down, restarts the system) when anomalies are discovered.	Interview officials and review related system documentation. Observe or test this system capability to determine that procedures are followed and related system documentation is generated and reviewed by entity security staff.

Source: GAO.

Critical Element CM-5. Update software on a timely basis to protect against known vulnerabilities

Software should be scanned and updated frequently to guard against known vulnerabilities. In addition to periodically looking for software vulnerabilities and fixing them, security software should be kept current by establishing effective programs for patch management, virus protection, and other emerging threats. Also, software releases should be adequately controlled to prevent the use of noncurrent software.

Exposure Draft

Vulnerability scanning

Using appropriate vulnerability scanning tools and techniques, entity management should scan for vulnerabilities in the information system or when significant new vulnerabilities affecting the system are identified and reported. Audit procedures include review of the scanning methodology and related results to ensure that significant vulnerabilities are remediated in a timely manner. (See section SM-5.1, table 9, for a description of vulnerability scanning.)

Patch management⁷⁹

Patch management is a critical process used to help alleviate many of the challenges involved with securing computing systems from attack. A component of configuration management, it includes acquiring, testing, applying, and monitoring patches to a computer system. Flaws in software code that could cause a program to malfunction generally result from programming errors that occur during software development. The increasing complexity and size of software programs contribute to the growth in software flaws. While most flaws do not create security vulnerabilities, the potential for these errors reflects the difficulty and complexity involved in delivering trustworthy code.

The federal government has taken several steps to address security vulnerabilities that affect agency systems, including efforts to improve patch management. Specific actions include (1) requiring agencies to annually report on their patch management practices as part of their implementation of FISMA, (2) identifying vulnerability remediation as a critical area of focus in the President's National Strategy to Secure Cyberspace, and (3) creating US-CERT.

- FISMA permanently authorized and strengthened the information security program, evaluation, and reporting requirements established for federal agencies in prior

⁷⁹Patch management is the process of applying software patches to correct flaws. A patch is a piece of software code that is inserted into a program to temporarily fix a defect. Patches are developed and released by software vendors when vulnerabilities are discovered.

Exposure Draft

legislation.⁸⁰ In accordance with OMB's reporting instructions for FISMA implementation, maintaining up-to-date patches is part of FISMA's system configuration management requirements.

- The President's National Strategy to Secure Cyberspace, issued on February 14, 2003, identifies priorities, actions, and responsibilities for the federal government as well as for state and local governments and the private sector. This strategy identifies the reduction and remediation of software vulnerabilities as a critical area of focus.
- The US-CERT is intended to aggregate and disseminate cybersecurity information to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection. Services include notification of software vulnerabilities and information on applicable patches.

Common patch management practices in security-related literature from several groups, including NIST, Microsoft, patch management software vendors, and other computer security experts include the following elements:

- centralized patch management support and clearly assigned responsibilities;
- senior executive support and assurance that appropriate patches are deployed;
- standardized patch management policies, procedures, and tools;
- skills, knowledge, and training to perform patch management responsibilities;
- current technology inventory of all hardware, software, and services that are used;
- risk assessment based on the criticality of the vulnerability and importance of the system;
- thorough testing before the patch is applied in a production environment;

⁸⁰Title X, Subtitle G—Government Information Security Reform, *Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001*, P.L. 106-398, October 30, 2000.

Exposure Draft

- monitoring through network and host vulnerability scanning; and
- timely notification of relevant vulnerabilities and distribution of critical patches.

Virus protection

Protecting information systems from malicious computer viruses and worms⁸¹ is a serious challenge. Computer attack tools and techniques are becoming increasingly sophisticated; viruses are spreading faster as a result of the increasing connectivity of today's networks; commercial-off-the-shelf products can be easily exploited for attack by all their users; and there is no "silver bullet" solution such as firewalls or encryption to protect systems. To combat viruses and worms specifically, entities should take steps such as ensuring that security personnel are adequately trained to respond to early warnings of attacks and keeping antivirus programs up-to-date. Strengthening intrusion detection capabilities and effective patch management programs also help.

According to NIST, the information system (including servers, workstations, and mobile computing devices) should implement malicious code protection that includes a capability for automatic updates. Virus definitions should be kept up-to-date. Virus-scanning software should be provided at critical entry points, such as remote-access servers and at each desktop system on the network. Anti-viral mechanisms should be used to detect and eradicate viruses in incoming and outgoing e-mail and attachments.

Emerging threats

Entities are facing a set of emerging cybersecurity threats that are the result of changing sources of attack, increasingly sophisticated social engineering techniques designed to trick the unsuspecting user into divulging sensitive information, new modes of covert compromise, and the blending of once distinct attacks into more complex and damaging exploits. Advances in antispyware measures

⁸¹Worms propagate through networks; viruses destroy files and replicate by manipulating files.

Exposure Draft

have caused spammers to increase the sophistication of their techniques to bypass detection; the frequency and sophistication of phishing⁸² attacks have likewise increased, and spyware⁸³ has proven to be difficult to detect and remove.

The risks that entities face are significant. Spam consumes employee and technical resources and can be used as a delivery mechanism for malware⁸⁴ and other cyberthreats. Entities and their employees can be victims of phishing scams, and spyware puts the confidentiality, integrity, and availability of entity systems at serious risk. Other emerging threats include the increased sophistication of worms, viruses, and other malware, and the increased attack capabilities of blended threats and botnets.⁸⁵

The transition to the new Internet protocol version 6 (IPv6) creates new security risks. The Internet protocol provides the addressing mechanism that defines how and where information moves across interconnected networks. The key characteristics of IPv6 are designed to increase address space, promote flexibility and functionality, and enhance security. However, as IPv6-capable software and devices accumulate in entity networks, they could be abused by attackers if not managed properly. Specifically, some existing firewalls and intrusion detection systems do not provide IPv6 detection or filtering capability, and malicious users might be able to send IPv6 traffic through these security devices undetected. Configuration management can mitigate this threat by tightening

⁸²Phishing is tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

⁸³Spyware is software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

⁸⁴Malware (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs so that users are induced into activating them. Malware can include viruses, worms, and spyware (GAO-05-231).

⁸⁵Botnets are compromised computers that can be remotely controlled by attackers to automatically launch attacks. Bots (short for robots) have become a key automation tool to speed the infection of vulnerable systems (GAO-05-231).

Exposure Draft

firewalls to deny direct outbound connections and tuning intrusion detection systems to detect IPv6 traffic.

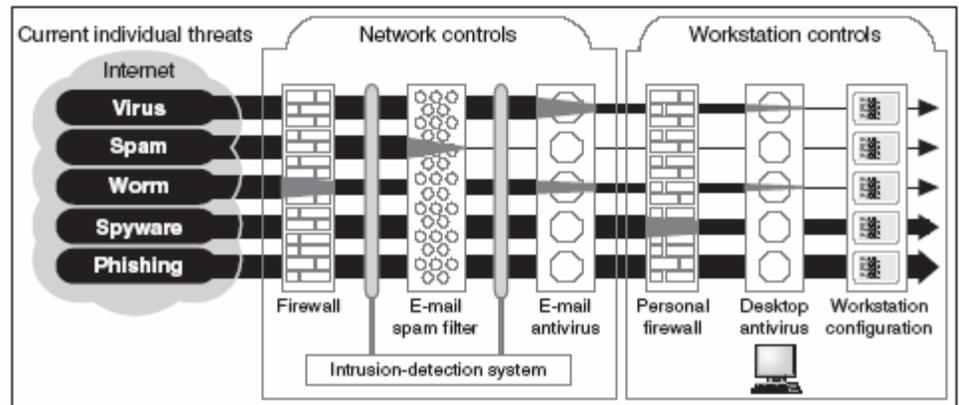
Voice over Internet Protocol (VoIP) technologies may also cause damage to the information system if used maliciously. To mitigate this threat, the entity should establish usage restrictions and implementation guidance for VoIP and document, monitor, and control the use of VoIP. NIST SP 800-58 provides guidance on security considerations for VOIP technologies employed in information systems.

An effective security program can assist in entity efforts to mitigate and respond to these emerging cybersecurity threats. First of all, the risks of emerging cybersecurity threats should be addressed as part of required entitywide information security programs, which include performing periodic assessments of risk. Secondly, security controls commensurate with the identified risk should be implemented. Thirdly, ensuring security awareness training for entity personnel is critical. Comprehensive procedures for detecting, reporting, and responding to security incidents should be implemented. An effective security program, related control techniques, and proposed audit procedures are discussed in the security management section of FISCAM.

As part of the entity security program, effective configuration of layered security (Defense-in-Depth) mitigates the risks from individual cybersecurity threats. Layered security implemented within an agency's security architecture includes the use of strong passwords, patch management, antivirus software, firewalls, software security settings, backup files, vulnerability assessments, and intrusion detection systems. Figure 5 depicts an example of how entities can use layered security controls to mitigate the risks of individual cybersecurity threats.

Exposure Draft

Figure 5. Layered Security Mitigates the Risk of Individual Cybersecurity Threats



Source: GAO.

Note: Excerpt from GAO, *Cybersecurity Issues Threaten Federal Information Systems*, GAO-05-231 (Washington, D.C.: May 2005).

Noncurrent software

Procedures should ensure that only current software releases are installed in information systems. Noncurrent software may be vulnerable to malicious code such as viruses and worms.

As mentioned previously under CM-3, many federal agencies have data processing operations that involve multiple locations and require a coordinated effort for effective and controlled distribution and implementation of new or revised software. This can include virus protection software and operating system patches. Once a modified software program has been approved for use, the change should be communicated to all affected parties and distributed and implemented in a way that leaves no doubt about when it is to begin affecting processing. Inadequately controlling virus software distribution and system patches increases the risk that data could be improperly processed or lose its confidentiality due to computer viruses and hackers breaking into the database.

Software usage

Policies and procedures should be implemented to reasonably assure that the entity complies with software usage restrictions. In addition, the entity should have policies and procedures implemented that address the installation of software by users and

Exposure Draft

procedures to determine that such policies and procedures are adhered to.

CM-5 Related NIST SP-800-53 Controls
 RA-5 Vulnerability Scanning
 SA-6 Software Usage Restrictions
 SA-7 User Installed Software
 SC-19 Voice Over Internet Protocol
 SI-2 Flaw Remediation
 SI-3 Malicious Code Protection
 SI-5 Security Alerts and Advisories
 SI-8 Spam Protection

Control Techniques and Suggested Audit Procedures for Critical Element CM-5

Table 27. Control Techniques and Suggested Audit Procedures for Critical Element CM-5: Update software on a timely basis to protect against known vulnerabilities

Control activities	Control techniques	Audit procedures
CM-5.1. Software is promptly updated to protect against known vulnerabilities.	CM-5.1.1. Information systems are scanned periodically to detect known vulnerabilities.	Interview entity officials. Identify the criteria and methodology used for scanning, tools used, frequency, recent scanning results, and related corrective actions. Coordinate this work with the AC section.
	CM-5.1.2. An effective patch management process is documented and implemented, including: <ul style="list-style-type: none"> • identification of systems affected by recently announced software vulnerabilities; • prioritization of patches based on system configuration and risk; • appropriate installation of patches on a timely basis, including testing for effectiveness and potential side effects on the agency's systems; and • verification that patches, service packs, and hotfixes were appropriately installed on affected systems. 	Review pertinent policies and procedures. Interview users and data processing staff.
	CM-5.1.3. Software is up-to-date; the latest versions of software patches are installed.	Compare vendor recommended patches to those installed on the system. If patches are not up-to-date, determine why they have not been installed.

Exposure Draft

Control activities	Control techniques	Audit procedures
	CM-5.1.4. An effective virus, spam, and spyware protection process is documented and implemented, including: <ul style="list-style-type: none"> • appropriate policies and procedures; • effective protection software is installed that identifies and isolates suspected viruses, spam, and spyware; and • virus, spam, and spyware definitions are up-to-date. 	Review pertinent policies and procedures. Interview users and data processing staff. Verify that actual software is installed and up-to-date.
	CM-5.1.5. The entity: (1) establishes usage restrictions and implementation guidance for IPv6 technology based on the potential to cause damage to the information system if used maliciously and (2) documents, monitors, and controls the use of IPv6 within the information system. Appropriate organizational officials authorize the use of IPv6.	Review policies and procedures for IPv6. Determine if known security vulnerabilities are mitigated by appropriate protective measures.
	CM-5.1.6. The entity: (1) establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously and (2) documents, monitors, and controls the use of VoIP within the information system. Appropriate organizational officials authorize the use of VoIP.	Review policies and procedures for VoIP. Determine if security considerations in NIST SP 800-58 are used in the information system.
	CM-5.1.7. Noncurrent software releases are adequately secure, given the risk.	Review pertinent policies and procedures. Interview users and data processing staff.
	CM-5.1.8. Appropriate software usage controls (software restrictions, user-installed software) are implemented and exceptions are identified.	Assess the adequacy of software usage controls.

Source: GAO.

Critical Element CM-6. Appropriately document and approve emergency changes to the configuration

Emergency changes to the information system should be documented and approved by appropriate entity officials, either before the change or after the fact. In addition, appropriate personnel should be notified to provide analysis and follow-up.

It is not uncommon for program changes to be needed on an emergency basis to keep a system operating. Some applications, such as payroll processing, are performed in cycles that must be completed by a deadline. Other systems must be continuously available so that the operations they support are not interrupted. In these cases, the risk of missing a deadline or disrupting operations may pose a greater risk than that of temporarily suspending program change controls. However, because of the increased risk

Exposure Draft

that errors or other unauthorized modifications could be implemented, emergency changes should be kept to a minimum.

It is important that an entity follow established procedures to perform emergency software changes and reduce the risk of suspending or abbreviating normal controls. Generally, emergency procedures should specify

- when emergency software changes are warranted,
- who may authorize emergency changes,
- how emergency changes are to be documented, and
- within what period after implementation the change must be tested and approved.

Making emergency changes often involves using sensitive system utilities or access methods that grant much broader access than would normally be needed. It is important that such access is strictly controlled and that their use be promptly reviewed.

Shortly after an emergency change is made, the usual configuration management controls should be applied retroactively. That is, the change should be subjected to the same review, testing, and approval process that applies to scheduled changes. In addition, logs of emergency changes and related documentation should be periodically reviewed by data center management or security administrators to determine whether all such changes have been tested and have received final approval.

Control Techniques and Suggested Audit Procedures for Critical Element CM-6

Table 28. Control Techniques and Suggested Audit Procedures for Critical Element CM-6: Appropriately document and approve emergency changes to the configuration

Control activities	Control techniques	Audit procedures
CM-6.1. Adequate procedures for emergency changes are documented and implemented.	CM-6.1.1. Appropriately document and implement procedures for emergency changes.	Review procedures.
CM-6.2. Emergency changes to the configuration are documented and approved.	CM-6.2.1. Appropriately document and approve emergency changes to the configuration and notify appropriate personnel for analysis and follow-up.	For a selection of emergency changes recorded in the emergency change log, review related documentation and approval.

Source: GAO.

Exposure Draft

3.4. Segregation of Duties (SD)

Effective segregation of duties starts with effective entitywide policies and procedures that are implemented at the system and application levels. Work responsibilities should be segregated so that one individual does not control all critical stages of a process. For example, while users may authorize program changes, programmers should not be allowed to do so because they are not the owners of the system and do not have the responsibility to see that the system meets user needs. Similarly, one computer programmer should not be allowed to independently write, test, and approve program changes. Often, segregation of duties is achieved by splitting responsibilities between two or more organizational groups. Dividing duties this way diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other.

Inadequately segregated duties, conversely, increase the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed. For example:

- An individual who is independently responsible for authorizing, processing, and reviewing payroll transactions could inappropriately increase payments to selected individuals without detection.
- A computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.

The extent to which duties are segregated depends on the size of the entity and the risk associated with its facilities and activities. A large entity will have more flexibility in separating key duties than will a small entity that must depend on only a few individuals to perform its operations. These smaller entities may rely more extensively on

Exposure Draft

supervisory review to control activities. Similarly, activities that involve extremely large dollar transactions or are otherwise inherently risky should be divided among several individuals and be subject to relatively extensive supervisory review.

Key areas of concern during a general controls review involve the segregation of duties among major operating and programming activities, including duties performed by users, application programmers, and data center staff. For example, where possible, the following types of activities should be separated: development versus production, security versus audit, accounts payable versus accounts receivable, and encryption key management versus the changing of keys. Entitywide policies outlining the responsibilities of groups and related individuals pertaining to incompatible activities should be documented, communicated, and enforced.

Because of the nature of computer operations, segregation of duties alone will not ensure that personnel perform only authorized activities, especially computer operators. Preventing or detecting unauthorized or erroneous personnel actions requires effective supervision and review by management and formal operating procedures.

Determining whether duties are adequately segregated and that the activities of personnel are adequately controlled involves assessing the agency's efforts in performing each of the critical elements listed in table 29.

<u>SD Related NIST SP-800-53 Controls</u>

AC-5 Separation of Duties

PS-2 Position Categorization

PS-6 Access Agreements

Exposure Draft

Table 29. Critical Elements for Segregation of Duties

Number	Description
SD-1.	Segregate incompatible duties and establish related policies
SD-2.	Control personnel activities through formal operating procedures, supervision, and review

Source: GAO

Critical Element SD-1. Segregate incompatible duties and establish related policies

The first steps in determining if duties are appropriately segregated are to analyze the agency's operations, identify incompatible duties, and assign these duties to different organizational units or individuals. Federal internal control standards specify that key duties and responsibilities for authorizing, processing, recording, and reviewing transactions should be separated. This concept can also be applied to the authorization, testing, and review of computer program changes.

Segregating duties begins by establishing independent organizational groups with defined functions, such as a payroll unit responsible for preparing payroll transaction input and a data processing unit responsible for processing input prepared by other units. Functions and related tasks performed by each unit should be documented for the unit and written in job descriptions and should be clearly communicated to personnel assigned the responsibilities.

Both physical and logical access controls can be used to enforce many entity policies regarding segregation of duties and should be based on organizational and individual job responsibilities. (Access control is discussed in detail in section 3.2.) For example, logical access controls can preclude computer programmers from using applications software or accessing computerized data associated with applications. Similarly, physical access controls, such as key cards and a security guard, can be used to prevent unauthorized individuals from entering a data processing center.

SD-1.1. Incompatible duties have been identified and policies implemented to segregate these duties
Management should have analyzed operations and identified incompatible duties that are then segregated through policies and organizational divisions. Although incompatible duties may vary

Exposure Draft

from one entity to another, the following functions are generally performed by different individuals: information security management, systems design, applications programming, systems programming, quality assurance and testing, library management/change management, computer operations, production control and scheduling, data security, data administration, network administration, and configuration management. A brief description of these functions follows.

Information security management includes the personnel who direct or manage the activities and staff of the information security department and its various organizational components.

Systems design is the function of identifying and understanding user information needs and translating them into a requirements document that is used to build a system.

Applications programming involves the development and maintenance of programs for specific applications, such as payroll, inventory control, accounting, and mission support systems.

Systems programming involves the development and maintenance of programs that form the system software, such as operating systems, utilities, compilers, and security software.

Quality assurance/testing involves the review and testing of newly-developed systems and modifications to determine whether they function as specified and perform in accordance with functional specifications. Testing may also determine whether appropriate procedures, controls, and documentation have been developed and implemented before approval is granted to place the system into operation.

Library management/change management is the control over program and data files that are either kept on-line or are on tapes and disks that are loaded onto the computer as needed. Software programs are generally used to assist in management of these files. This function also is often responsible for controlling documentation related to system software, application programs, and computer operations.

Exposure Draft

Computer operations involves performing the various tasks to operate the computer and peripheral equipment, including providing the tape, disk, or paper resources as requested by the applications systems.

Production control and scheduling involves monitoring the information into, through, and as it leaves the computer operations area, and for determining the succession of programs to be run on the computer. Often, an automated scheduling package is used in this task. An entity may have a separate data control group that is responsible for seeing that all data necessary for processing are present and that all output is complete and distributed properly. This group is usually also responsible for reconciling record counts and control totals submitted by users with similar counts and totals generated during processing.

The data security function in an IT department involves the development and administration of an agency's information security program. This includes development of security policies, procedures, and guidelines and the establishment and maintenance of a security awareness and education program for employees. This function is also concerned with the adequacy of access controls and service continuity procedures.

Data administration involves planning for and administering the data used throughout the entity. This function is concerned with identifying, cataloging, controlling, and coordinating the information needs of the entity. Database administration is a narrower function concerned with the technical aspects of installing, maintaining, and using an agency's databases and database management systems.

Network administration involves maintaining a secure and reliable on-line communications network and serving as liaison with user departments to resolve network needs and problems.

Configuration management involves controlling and documenting changes made to a system's hardware, software, firmware, and documentation throughout the development and operational life of the system.

Exposure Draft

The following include examples of restrictions that are generally addressed in policies about segregating duties and are achieved through organizational divisions and access controls:

- Application users should not have access to operating systems or applications software.
- Programmers should not be responsible for moving programs into production or have access to production libraries or data.
- Access to operating system documentation should be restricted to authorized systems programming personnel.
- Access to applications system documentation should be restricted to authorized applications programming personnel.
- Access to production software libraries should be restricted to library management personnel.
- Persons other than computer operators should not set up or operate the production computer.
- Only users—not computer staff—should be responsible for transaction origination or correction and for initiating changes to application files.
- Computer operators should not have access to program libraries or data files.

Some steps involved in processing a transaction also need to be separated among different individuals. For example, the following combinations of functions should not be performed by a single individual:

- Data entry and verification of data.
- Data entry and its reconciliation to output.
- Input of transactions for incompatible processing functions (for example, input of vendor invoices and purchasing and receiving information).
- Data entry and supervisory authorization functions (for example, authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's review and approval).

Exposure Draft

Organizations with limited resources to segregate duties should have compensating controls, such as supervisory review of transactions performed.

SD-1.2. Job descriptions have been documented

Documented job descriptions should exist that clearly describe employee duties and prohibited activities. These should include responsibilities that may be assumed during emergency situations. The documented job descriptions should match employees' assigned duties. Also, they should include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position, and should be useful for hiring, promoting, and performance evaluation purposes. In addition, the organization should assign a risk designation to all positions and establish screening criteria for individuals filling those positions.

SD-1.3. Employees understand their duties and responsibilities

Employees and their supervisors should understand their responsibilities and the activities that are prohibited. Ultimate responsibility for this rests with senior managers. They should provide the resources and training so that employees understand their responsibilities and ensure that segregation-of-duties principles are established, enforced, and institutionalized within the organization.

Control Techniques and Suggested Audit Procedures for Critical Element SD-1

Table 30. Control Techniques and Suggested Audit Procedures for Critical Element SD-1: Segregate incompatible duties and establish related policies

Control activities	Control techniques	Audit procedures
SD-1.1. Incompatible duties have been identified and policies implemented to segregate these duties.	SD-1.1.1. Policies and procedures for segregating duties exist and are up-to-date.	Review pertinent policies and procedures. Interview selected management and information security personnel regarding segregation of duties.

Exposure Draft

Control activities	Control techniques	Audit procedures
	<p>SD-1.1.2. Distinct system support functions are performed by different individuals, including the following:</p> <ul style="list-style-type: none"> • information security management • systems design • applications programming • systems programming • quality assurance/testing • library management/change management • computer operations • production control and scheduling • data control • data security • data administration • network administration • configuration management 	<p>Review an entity organization chart showing information security functions and assigned personnel.</p> <p>Interview selected personnel and determine whether functions are appropriately segregated.</p> <p>Determine whether the chart is current and each function is staffed by different individuals.</p> <p>Review relevant alternate or back up assignments and determine whether the proper segregation of duties is maintained.</p> <p>Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.</p>
	<p>SD-1.1.3. No individual has complete control over incompatible transaction processing functions. Specifically, the following combination of functions are not performed by a single individual:</p> <ul style="list-style-type: none"> • data entry and verification of data • data entry and its reconciliation to output • input of transactions for incompatible processing functions (for example, input of vendor invoices and purchasing and receiving information) • data entry and supervisory authorization functions (for example, authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's review and approval) 	<p>Review the organizational chart and interview personnel to determine that assignments do not result in a single person being responsible for the indicated combinations of functions.</p> <p>Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.</p>
	<p>SD-1.1.4. Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.</p>	<p>Interview management, observe activities, and test transactions. Note: Perform this in conjunction with SD-2.2.</p>
	<p>SD-1.1.5. Data processing personnel are not users of information systems. They and security managers do not initiate, input, or correct transactions.</p>	<p>Determine through interview and observation whether data processing personnel and security managers are prohibited from these activities.</p>
	<p>SD-1.1.6. Day-to-day operating procedures for the data center are adequately documented and prohibited actions are identified.</p>	<p>Review the adequacy of documented operating procedures for the data center.</p>
	<p>SD-1.1.7. Access controls enforce segregation of duties.</p>	<p>Audit procedures are found in section AC-3.1, but this item is listed here as a reminder. Logical and physical access controls should enforce segregation of duties.</p>

Exposure Draft

Control activities	Control techniques	Audit procedures
SD-1.2. Job descriptions have been documented.	SD-1.2.1. Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.	Review job descriptions for several positions in organizational units and for user security administrators. Determine whether duties are clearly described and prohibited activities are addressed. Review the effective dates of the position descriptions and determine whether they are current. Compare these descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.
	SD-1.2.2. Documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and can be used for hiring, promoting, and performance evaluation purposes.	Review job descriptions and interview management personnel.
SD-1.3. Employees understand their duties and responsibilities.	SD-1.3.1. All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.	Interview personnel filling positions for the selected job descriptions (see SD-1.2). Determine if the descriptions match their understanding of their duties and responsibilities and whether additional duties are undertaken that are not listed in their job descriptions.
	SD-1.3.2. Senior management is responsible for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization.	Determine from interviewing personnel whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.
	SD-1.3.3. Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood, and followed.	Interview management personnel in these activities.

Source: GAO.

Critical Element SD-2. Control personnel activities through formal operating procedures, supervision, and review

Control over personnel activities requires formal operating procedures and active supervision and review of these activities. This is especially relevant for computer operators and system administrators. Some information system officials have extensive access rights in order to keep the systems running efficiently so their activities need to be monitored closely. Inadequacies in this area could allow mistakes to occur and go undetected and facilitate unauthorized use of the computer.

Exposure Draft

SD-2.1. Formal procedures guide personnel in performing their duties

Detailed, written instructions should be followed to guide personnel in performing their duties. These instructions are especially important for computer operators. For example, computer operator instruction manuals should provide guidance on system start up and shut down procedures, emergency procedures, system and job status reporting, and operator-prohibited activities. Application-specific manuals (commonly called run manuals) should provide additional instructions for operators specific to each application, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures. Operators should be prevented from overriding file label or equipment error messages.

SD-2.2. Active supervision and review are provided for all personnel

Supervision and review of personnel computer systems activities help make certain that these activities are performed in accordance with prescribed procedures, that mistakes are corrected, and that the computer is used only for authorized purposes. To aid in this oversight, all user activities on the computer system should be recorded on activity logs, which serve as an audit trail. Supervisors should routinely review these activity logs for incompatible actions and investigate any abnormalities.

Periodic management reviews of computer systems activities are essential to ensure that employees are performing their duties in accordance with established policies and to identify the need to update policies when operational processes change. In particular, management should periodically review activities that cannot be controlled by physical or logical access controls. Such activities are typically controlled instead by supervisory oversight and documentation showing approvals and authorizations.

Exposure Draft

Control Techniques and Suggested Audit Procedures for Critical Element SD-2

Table 31. Control Techniques and Suggested Audit Procedures for Critical Element SD-2: Control personnel activities through formal operating procedures, supervision, and review

Control activities	Control techniques	Audit procedures
SD-2.1. Formal procedures guide personnel in performing their duties.	SD-2.1.1. Detailed, written instructions exist and are followed for the performance of work.	Review manuals.
	SD-2.1.2. Instruction manuals provide guidance on system operation.	Interview supervisors and personnel. Observe processing activities.
	SD-2.1.3. Application run manuals provide instruction on operating specific applications.	
SD-2.2. Active supervision and review are provided for all personnel.	SD-2.2.1. Personnel are provided adequate supervision and review, including each shift for computer operations.	Interview supervisors and personnel. Observe processing activities.
	SD-2.2.2. Access authorizations are periodically reviewed for incompatible functions.	Review sample of access authorizations for incompatible functions and evidence of supervisory review.
	SD-2.2.3. Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (for example, periodic risk assessments).	Determine which reviews are conducted to assess the adequacy of duty segregation. Obtain and review results of such reviews. Note: This audit step should be performed in conjunction with audit steps in critical elements SM-2 (Periodically assess and validate risks) and SM-5 (Monitor the effectiveness of the security program).
	SD-2.2.4. Staff performance is monitored on a periodic basis and controlled to ensure that objectives laid out in job descriptions are carried out.	Interview management and subordinate personnel. Select documents or actions requiring supervisory review and approval for evidence of such performance (for example, approval of input of transactions, software changes).
	SD-2.2.5. Supervisors routinely review user activity logs for incompatible actions and investigate any abnormalities.	Interview supervisors and review user activity logs for incompatible actions. Check for evidence of supervisory review.

Source: GAO.

Exposure Draft

3.5. Contingency Planning (CP)

Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an agency's ability to accomplish its mission. If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. For some operations, such as those involving health care or safety, system interruptions could even result in injuries or loss of life.

Given these severe implications, it is critical that an entity have in place (1) procedures for protecting information resources and minimizing the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. Such plans should consider the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as those performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster-simulation exercises. FISMA requires that each federal agency implement an information security program that includes "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."

Although often referred to as disaster recovery or contingency plans, controls to ensure service continuity should address the entire range of potential disruptions. These may include relatively minor interruptions, such as temporary power failures, as well as major disasters, such as fires, natural disasters, and terrorism, that would require reestablishing operations at a remote location; it might also include errors, such as writing over a file. If controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data.

To mitigate service interruptions, it is essential that the related controls be understood and supported by management and staff throughout the entity. Senior management commitment is especially important to ensuring that adequate resources are devoted to

Exposure Draft

emergency planning, training, and related testing. Also, the involvement of data and process owners is integral to contingency planning, as they have first-hand knowledge of their data and processes and of the impact of a loss of availability. In addition, all staff with contingency planning responsibilities, such as those responsible for backing up files, should be fully aware of the risks of not fulfilling those duties.

Assessing contingency planning controls involves evaluating the agency's performance in each of the critical elements listed in table 32.

Table 32. Critical Elements for Contingency Planning

Number	Description
CP-1.	Assess the criticality and sensitivity of computerized operations and identify supporting resources
CP-2.	Take steps to prevent and minimize potential damage and interruption
CP-3.	Develop and document a comprehensive contingency plan
CP-4.	Periodically test the contingency plan and adjust it as appropriate

Source: GAO

Critical Element CP-1. Assess the criticality and sensitivity of computerized operations and identify supporting resources

At most entities, the continuity of certain automated operations is more important than for other operations, and it is not cost effective to provide the same level of continuity for all operations. For this reason, it is important that management analyze data and operations to determine which are the most critical and what resources are needed to recover and support them. This is the first step in determining which resources merit the greatest protection and what contingency plans need to be made.

As explained in SM-2, FISMA required NIST to develop standards and guidelines for agencies to use in categorizing federal information and information systems so agencies can provide the appropriate level of information security according to a range of risks. This information is useful in assessing risks and the criticality and sensitivity of computerized operations, and in identifying

Exposure Draft

supporting resources. It is also very important to link this information to the agency's mission and critical business processes.

According to NIST, the definition of an organization's critical mission or business functions is often called a business plan, and it is used to support contingency planning.⁸⁶ Part of business planning involves the development of a business continuity plan that focuses on sustaining an organization's business functions during and after a disruption. A business continuity plan can be written for a specific business process or it may address all key business processes. Because there is an inherent relationship between an IT system and the business process it supports, there should be coordination between each plan, and ultimately an entity may use a suite of plans for its IT systems, business processes, and the facility.⁸⁷ In addition, a business impact analysis should be conducted to (1) identify critical information technology resources, (2) identify outage impact and allowable outage times, and (3) develop recovery priorities. The purpose of the business impact analysis is to correlate specific system components with the critical services that they provide and, based on that information, to characterize the consequences if system components were to be disrupted.

CP-1.1. Critical data and operations are identified and prioritized

The criticality and sensitivity of various data and operations should be determined and prioritized based on security categorizations and an overall risk assessment of the agency's operations. As discussed in section 3.1, Entitywide Security Management Program, such a risk assessment should serve as the foundation of an agency's security plan. Factors to be considered include the importance and sensitivity of the data and other organizational assets handled or protected by the individual operations, and the cost of not restoring data or operations promptly. For example, a 1-day interruption of

⁸⁶NIST, *An Introduction to Computer Security: The NIST Handbook*, Special Publication (SP) 800-12, October 1995.

⁸⁷ NIST, *Contingency Planning Guide for Information Technology Systems*, Special Publication (SP) 800-34, June 2002.

Exposure Draft

major tax or fee-collection systems or a loss of related data could significantly slow or halt receipt of revenues, diminish controls over millions of dollars in receipts, and reduce public trust. Conversely, a system that monitors employee training could be out of service for perhaps as much as several months without serious consequences. Further, sensitive data, such as personal information on individuals or information related to contract negotiations, may require special protection during a suspension of normal service, even if such information is not needed on a daily basis to carry out critical operations.

Generally, critical data and operations should be identified and ranked by those personnel involved in the agency's business or program operations. For example, managers should predict the negative effects of lost data and interrupted operations and determine how long specific operations can be suspended or postponed. However, it is also important to obtain senior management's agreement with such determinations, as well as concurrence from affected groups.

The prioritized listing of critical information resources and operations should be periodically reviewed to determine whether current conditions are reflected in it. Such reviews should occur whenever there is a significant change in the agency's mission and operations or in the location or design of the systems that support these operations.

CP-1.2. Resources supporting critical operations are identified and analyzed

Once critical data and operations have been determined, the minimum resources needed to support them should be identified and their roles analyzed. The resources to be considered include computer resources, such as hardware, software, and data files; networks, including components such as routers and firewalls; supplies, including paper stock and preprinted forms; telecommunications services; and any other resources that are necessary to the operation, such as people, office facilities and supplies, and noncomputerized records. For example, an analysis should be performed to identify the maximum number of disk drives needed at one time and the specific requirements for telecommunications lines and devices.

Exposure Draft

Because essential resources are likely to be held or managed by a variety of groups within an entity, it is important that program and information security support staff work together to identify the resources needed for critical operations.

CP-1.3. Emergency processing priorities are established

In conjunction with identifying and ranking critical functions, the entity should develop a plan for restoring critical operations. The plan should clearly identify the order in which various aspects of processing should be restored, who is responsible, and what supporting equipment or other resources will be needed. A carefully developed processing restoration plan can help employees immediately begin the restoration process and make the most efficient use of limited computer resources during an emergency. Both system users and information security support staff should be involved in determining emergency processing priorities. (See critical element CP-3 for additional information on contingency planning.)

Control Techniques and Suggested Audit Procedures for Critical Element CP-1

Table 33. Control Techniques and Suggested Audit Procedures for Critical Element CP-1: Assess the criticality and sensitivity of computerized operations and identify supporting resources

Control activities	Control techniques	Audit procedures
CP-1.1. Critical data and operations are identified and prioritized.	CP-1.1.1. The entity categorizes information systems in accordance with appropriate guidance, such as FIPS 199, and documents the results in the system security plan. CP-1.1.2 A list of critical operations and data has been documented that <ul style="list-style-type: none">• identifies primary mission or business functions,• prioritizes data and operations,• is approved by senior program managers, and• reflects current conditions including system interdependencies and technologies.	Review the policies and methodology used to categorize systems and create the critical operations list. This list should identify each system and its criticality in supporting the agency's primary mission or business functions. Review how systems are categorized and the critical operations list. Determine if the justifications have been documented and that they (1) prioritize data and operations by primary mission or business functions; (2) are approved by senior management; and (3) reflect current operating conditions, including key system interdependencies. Determine if technology supporting critical operations is identified and appropriately considered in processing priorities. Interview program, information technology, and security administration officials. Determine their input and assessment of the reasonableness of priorities established.

Exposure Draft

Control activities	Control techniques	Audit procedures
CP-1.2. Resources supporting critical operations are identified and analyzed.	CP-1.2.1. Resources supporting critical operations and functions have been identified and documented. Types of resources identified should include <ul style="list-style-type: none"> • computer hardware, • computer software, • computer supplies, • network components, • system documentation, • telecommunications, • office facilities and supplies, and • human resources. 	Interview program and security administration officials responsible for developing the critical operations listing. Review documentation supporting the critical operations listing to verify that the following resources have been identified for each critical operation: <ul style="list-style-type: none"> • computer hardware and software, • computer supplies, • network components, • system documentation, • telecommunications, • office facilities and supplies, and • human resources. Appropriate documentation may include contingency-related plans in NIST SP 800-34.
	CP-1.2.2. Critical information technology resources have been analyzed to determine their impact on operations if a given resource were disrupted or damaged. This analysis should evaluate the impact of the outages over time and across related resources and dependent systems.	Determine if a current business impact analysis has been conducted that identifies critical information technology resources, disruption impacts, allowed outage times, and recovery priorities.
CP-1.3. Emergency processing priorities are established.	CP-1.3.1. Emergency processing priorities have been documented and approved by appropriate program and data processing managers.	Review related policies, plans, and procedures for emergency processing and ensure: <ul style="list-style-type: none"> • recovery priorities have been developed, • management has approved priorities, and • priorities are documented. Request a copy of the continuity of operations plan. Interview program and security administration officials to determine whether they are aware of all policies and procedures for emergency processing priorities and maintain copies of the continuity of operations plan.

Source: GAO.

Critical Element CP-2. Take steps to prevent and minimize potential damage and interruption

There are a number of steps that an entity should take to prevent or minimize the damage to automated operations that can occur from unexpected events. These can be categorized as

- routinely duplicating or backing up data files, computer programs, and critical documents with off-site storage;

Exposure Draft

- arranging for remote backup facilities that can be used if the agency's usual facilities are damaged beyond use;
- establishing an information system recovery and reconstitution capability so that the information system can be recovered and reconstituted to its original state after a disruption or failure;
- installing environmental controls, such as fire-suppression systems or backup power supplies; and
- ensuring that staff and other system users understand their responsibilities during emergencies.

Such steps, especially implementing thorough backup procedures and installing environmental controls, are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters. In particular, an entity should maintain an ability to restore data files, which may be impossible to recreate if lost. In addition, effective maintenance, problem management, and change management for hardware equipment will help prevent unexpected interruptions.

In an IS controls audit being performed as part of a financial audit or data reliability assessment, the auditor should tailor the identification of control techniques and audit procedures related to environmental controls (CP-2.2) and hardware maintenance (CP-2.4) to achieve the audit objectives, considering the IS controls identified by the auditor as significant to the audit objectives (e.g., internal control over financial reporting).

CP-2.1. Data and program backup procedures have been implemented

Routinely copying data files and software and storing these files at a secure, remote location are usually the most cost-effective actions that an entity can take to mitigate service interruptions. Although equipment can often be readily replaced, the cost could be significant and reconstructing computerized data files and replacing software can be extremely costly and time consuming. And, data files cannot always be reconstructed. In addition to the direct costs of reconstructing files and obtaining software, the related service interruptions could lead to significant financial losses.

Exposure Draft

A program should be in place for regularly backing up computer files, including master files, transaction files, application programs, system software, and database software, and for storing these backup copies securely at an off-site location. Choosing a location depends on the particular needs of the entity, but in general, the location should be far enough away from the primary location that it will be protected from events such as fires, storms, electrical power outages, and terrorism that may occur to the primary location. In addition, it should be protected from unauthorized access and from environmental hazards.

The frequency with which files should be backed up depends on the volume and timing of transactions that modify the data files. Generally, backing up files on a daily basis is adequate. However, if a system accounts for thousands of transactions per day, it may be appropriate to back up files several times a day. Conversely, if only a few transactions are recorded every week, then weekly backing up of files may be adequate.

File back up procedures should be designed so that a recent copy is always available. For example, new data file versions should be received at the off-site storage location before the disks or tapes containing prior versions are returned to the data center for reuse.

Generally, data center personnel are responsible for routinely backing up files. However, if critical data are routinely maintained on computers that are not under the control of data center personnel, then responsibility for backing up this information should be clearly defined.

In addition to data files and software programs, copies of any other information and supplies that may be needed to maintain operations should be maintained at a remote location. Examples of such documents are system and application documentation, unique preprinted computer paper, and essential legal files. Although a review of computer-related controls focuses on electronically maintained data, it is important that critical paper documents also be copied and stored remotely so that they are available when needed to support automated operations.

Exposure Draft

CP-2.2. Adequate environmental controls have been implemented

Environmental controls prevent or mitigate potential damage to facilities and interruptions in service. Examples of environmental controls include

- fire extinguishers and fire-suppression systems;
- fire alarms;
- smoke detectors;
- water detectors;
- emergency lighting;
- redundancy in air cooling systems;
- backup power supplies;
- existence of shut-off valves and procedures for any building plumbing lines that may endanger processing facilities;
- processing facilities built with fire-resistant materials and designed to reduce the spread of fire; and
- policies prohibiting eating, drinking, and smoking within computer facilities.

Environmental controls can diminish the losses from some interruptions such as fires or prevent incidents by detecting potential problems early, such as water leaks or smoke, so that they can be remedied. Also, uninterruptible or backup power supplies can carry a facility through a short power outage or provide time to back up data and perform orderly shut-down procedures during extended power outages.

CP-2.3. Staff have been trained to respond to emergencies

Staff should be trained in and aware of their responsibilities in preventing, mitigating, and responding to emergency situations. For example, information security support staff should receive periodic training in emergency fire, water, and alarm incident procedures, as well as in their responsibilities in starting up and running an alternate data processing site. Also, if outside users are critical to the agency's operations, they should be informed of the steps they may have to take as a result of an emergency.

Exposure Draft

Generally, information on emergency procedures and responsibilities can be provided through training sessions and by distributing written policies and procedures. Training sessions should be held at least once a year and whenever changes to emergency plans are made. Further, if staff could be required to relocate or significantly alter their commuting routine in order to operate an alternate site in an emergency, it is advisable for an entity to incorporate into the contingency plan steps for arranging lodging and meals or any other facilities or services that may be needed to accommodate essential personnel.

CP-2.4. Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions

Unexpected service interruptions can occur from hardware equipment failures or from changing equipment without adequate advance notification to system users. To prevent such occurrences requires an effective program for maintenance, problem management, and change management for hardware equipment.

Routine periodic hardware maintenance should be scheduled and performed to help reduce the possibility and impact of equipment failures. Vendor-supplied specifications normally prescribe the frequency and type of preventive maintenance to be performed. Such maintenance should be scheduled in a manner to minimize the impact on overall operations and on critical or sensitive applications. Specifically, peak workload periods should be avoided. All maintenance performed should be documented, especially any unscheduled maintenance that could be analyzed to identify problem areas warranting additional action for a more permanent solution. Flexibility should be designed into the data processing operations to accommodate the required preventive maintenance and reasonably expected unscheduled maintenance. For critical or sensitive applications that require a high level of system availability, the acquisition and use of spare or backup hardware may be appropriate.

Effective problem management requires tracking service performance and documenting problems encountered. Goals should be established by senior management on the availability of data processing and on-line service. Records should be maintained on the

Exposure Draft

actual performance in meeting service schedules. Problems and delays encountered, the reasons for the problems or delays, and the elapsed time for resolution should be recorded and analyzed to identify any recurring pattern or trend. Senior management should periodically review and compare the service performance achieved with the goals and survey user departments to see if users' needs are being met.

Changes to hardware equipment and related software should be scheduled to minimize the impact on operations and users and allow for adequate testing to demonstrate that they will work as expected. Advance notification should be given to users so that service is not unexpectedly interrupted.

CP-2 Related NIST SP-800-53 Controls

- CP-3 Contingency Training
- CP-6 Alternative Storage Site
- CP-7 Alternate Processing Site
- CP-9 Information System Backup
- CP-10 Information System Recovery and Reconstitution
- MA-2 Controlled Maintenance
- MA-3 Maintenance Tools
- MA-5 Maintenance Personnel
- MA-6 Timely Maintenance
- PE-9 Power Equipment and Power Cabling
- PE-10 Emergency Shutoff
- PE-11 Emergency Power
- PE-12 Emergency Lighting
- PE-13 Fire Protection
- PE-14 Temperature and Humidity Controls
- PE-15 Water Damage Protection
- PE-16 Delivery and Removal
- PE-17 Alternate Work Site
- PE-18 Location of Information System Components
- SA-5 Information System Documentation

Exposure Draft

Control Techniques and Suggested Audit Procedures for Critical Element CP-2

Table 34. Control Techniques and Suggested Audit Procedures for Critical Element CP-2: Take steps to prevent and minimize potential damage and interruption

Control activities	Control techniques	Audit procedures
CP-2.1. Information system back up and recovery procedures have been implemented.	CP-2.1.1. Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.	Review written policies and procedures for backing up and transporting files. Determine how often files are backed up and rotated off site, retention periods, and security involved in transport. Compare inventory records with the files maintained off-site and determine the age of these files. For a selection of critical files, locate and examine the backup files. Verify that backup files can be used to recreate current reports. Determine whether backup files are created and rotated off-site as prescribed and are sent before prior versions are returned. Determine if the technology is implemented in such a manner as to provide appropriate availability, including consideration of backup procedures, system configuration, redundancy, environmental controls, staff training, and routine maintenance.
	CP-2.1.2. System and application documentation is maintained at the off-site storage location.	Locate and examine documentation.
	CP-2.1.3. The backup storage site is <ul style="list-style-type: none"> geographically removed from the primary site (for example, not subject to the same hazards), and protected by environmental controls and physical access controls. 	Examine the backup storage site. Determine if there are accessibility problems between the storage and processing sites in the event of an area wide disaster.
	CP-2.1.4. The information system back up and recovery procedures adequately provide for recovery and reconstitution to the system's original state after a disruption or failure including <ul style="list-style-type: none"> system parameters are reset; patches are reinstalled; configuration settings are reestablished; system documentation and operating procedures are available; application and system software is reinstalled; information from the most recent backup is available; and the system is fully tested. 	Interview entity officials and determine whether comprehensive procedures and mechanisms exist to fully restore the information security to its original state. Determine if this recovery capability has been tested and, if so, review the test plan and test results.
CP-2.2. Adequate environmental controls have been implemented.		These procedures should be performed in conjunction with Section AC-6 regarding physical access controls.

Exposure Draft

Control activities	Control techniques	Audit procedures
	<p>CP-2.2.1. Fire detection and suppression devices have been installed and are working, for example, smoke detectors, fire extinguishers, and sprinkler systems.</p> <p>CP-2.2.2. Controls have been implemented to mitigate other disasters, such as floods, earthquakes, terrorism, etc.</p> <p>CP-2.2.3. Redundancy exists in critical systems (for example, power and air cooling systems)</p> <p>CP-2.2.4. Building plumbing lines do not endanger the computer facility or, at a minimum, shut-off valves and procedures exist and are known.</p> <p>CP-2.2.5. An uninterruptible power supply or backup generator has been provided so that power will be adequate for orderly shut down.</p> <p>CP-2.2.6. Humidity, temperature, and voltage are controlled within acceptable levels.</p> <p>CP-2.2.7. Emergency lighting activates in the event of a power outage and covers emergency exits and evacuation routes.</p> <p>CP-2.2.8. A master power switch or emergency shut-off switch is present and appropriately located.</p> <p>CP-2.2.9. Environmental controls are periodically tested at least annually for federal agencies</p>	<p>Examine the agency's facilities.</p> <p>Interview site managers.</p> <p>Observe that operations staff are aware of the locations of fire alarms, fire extinguishers, regular and auxiliary electrical power switches, water shut-off valves, breathing apparatus, and other devices that they may be expected to use in an emergency. Also, observe that emergency lighting works and that power and other cabling is protected.</p> <p>Observe the operation, location, maintenance, and access to the air cooling systems. Determine whether humidity, temperature, and voltage are appropriately controlled.</p> <p>Observe whether water can enter through the computer room ceiling or whether pipes are running through the facility and that there are water detectors on the floor.</p> <p>Determine whether the activation of heat and smoke detectors will notify the fire department.</p> <p>Review test policies.</p> <p>Review documentation supporting recent tests of environmental controls.</p>
<p>CP-2.3. Staff have been trained to respond to emergencies.</p>	<p>CP-2.3.1. Operational and support personnel have received training and understand their emergency roles and responsibilities.</p> <p>CP-2.3.2. Personnel receive periodic environmental controls training including emergency fire, water, and alarm incident procedures.</p> <p>CP-2.3.3. Emergency response procedures are documented.</p> <p>CP-2.3.4. Emergency procedures are periodically tested.</p>	<p>Review policies and procedures regarding employee behavior.</p> <p>Observe employee behavior.</p> <p>Interview security personnel and appropriate operational and support staff and ensure that they understand their roles and responsibilities.</p> <p>Review training records and training course documentation. Determine whether all personnel have received up-to-date training and that the scope of the training is adequate.</p> <p>Review emergency response procedures for completeness and determine whether roles and responsibilities are clearly defined.</p> <p>Review test policies.</p> <p>Review test documentation.</p> <p>Interview operational and data center staff.</p>
<p>CP-2.4. Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.</p>	<p>CP-2.4.1. Policies and procedures exist and are up-to-date.</p>	<p>Review policies and procedures.</p>

Exposure Draft

Control activities	Control techniques	Audit procedures
	CP-2.4.2. Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations.	Interview information security, data processing, and user management. Review maintenance documentation.
	CP-2.4.3. Regular and unscheduled maintenance performed is documented.	Determine when maintenance is performed, if it is in accordance with vendor specifications, and if there is minimal impact on system availability.
	CP-2.4.4. Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled maintenance.	
	CP-2.4.5. Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.	Interview information security and data center management.
	CP-2.4.6. Goals are established by senior management on the availability of data processing and on-line services.	Interview senior management, information security management, data processing management, and user management.
	CP-2.4.7. Records are maintained on the actual performance in meeting service schedules.	Review supporting documentation, including system performance metrics.
	CP-2.4.8. Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.	
	CP-2.4.9. Senior management periodically reviews and compares the service performance achieved with the goals and surveys of user departments to see if their needs are being met.	Interview senior management, information security management, data processing management, and user management.
	CP-2.4.10. Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing.	Review supporting documentation such as user surveys, service goals, metrics measuring system availability, service schedules, and test plans.
	CP-2.4.11. Advance notification of hardware changes is given to users so that service is not unexpectedly interrupted.	

Source: GAO.

Critical Element CP-3. Develop and document a comprehensive contingency plan

A contingency plan or suite of related plans should be developed for restoring critical applications; this includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. Agency/entity-level policies and procedures define the contingency planning process and documentation requirements. Furthermore, an entitywide plan should identify critical systems, applications, and any subordinate or related plans. It is important that these plans be clearly documented, communicated to affected staff, and updated to reflect current operations. Testing the plan is addressed in critical element

Exposure Draft

CP-4. In addition, the plan should address entity systems maintained by a contractor or other entity (e.g., through service level agreements).

According to NIST, contingency planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency. IT contingency planning fits into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning. Ultimately, an organization may use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's IT systems, business processes, and the facility. Because there is an inherent relationship between an IT system and the business process it supports, there should be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

The NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, discusses the types of contingency plans that an organization might use and how they relate to each other. Since there is no standard definition for these plans, they may vary from organization to organization. To provide a common basis of understanding for IT contingency planning, NIST developed the descriptions shown in the table below.

Table 35: Types of Contingency-Related Plans

Plan	Purpose	Scope
Business Continuity Plan (BCP)	Provide procedures for sustaining essential business operations while recovering from a significant disruption	Addresses business processes; IT addressed based only on its support for business process
Business Recovery (or Resumption) Plan (BRP)	Provide procedures for recovering business operations immediately following a disaster	Addresses business processes; not IT-focused; IT addressed based only on its support for business process

Exposure Draft

Continuity of Operations Plan (COOP)	Provide procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days	Addresses the subset of an organization's missions that are deemed most critical; usually written at headquarters level; not IT-focused
Continuity of Support Plan/IT Contingency Plan	Provide procedures and capabilities for recovering a major application or general support system	Same as IT contingency plan; addresses IT system disruptions; not business process focused
Crisis Communications Plan	Provides procedures for disseminating status reports to personnel and the public	Addresses communications with personnel and the public; not IT focused
Cyber Incident Response Plan	Provide strategies to detect, respond to, and limit consequences of malicious cyber incident	Focuses on information security responses to incidents affecting systems and/or networks
Disaster Recovery Plan (DRP)	Provide detailed procedures to facilitate recovery of capabilities at an alternate site	Often IT-focused; limited to major disruptions with long-term effects
Occupant Emergency Plan (OEP)	Provide coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat	Focuses on personnel and property particular to the specific facility; not business process or IT system functionality based

Source: NIST Contingency Planning Guide for Information Technology Systems (SP 800-34).

In addition, NIST addresses technical contingency planning considerations and solutions for specific information technology platforms: (1) desktop computers and portable systems, (2) servers, (3) Web sites, (4) local area networks, (5) wide area networks, (6) distributed systems, and (7) mainframe systems.

Note that incident handling can be considered that portion of contingency planning that responds to malicious technical threats. An incident response capability is addressed in critical element AC-5.1.

CP-3.1. An up-to-date contingency plan is documented

Contingency plans should be documented, agreed on by both users and information security departments, and communicated to

Exposure Draft

affected staff. FISMA requires that each federal agency develop, document, and implement an agencywide information security program that includes plans to ensure continuity of operations for information systems.

The plan should reflect the risks and operational priorities that the entity has identified. It should be designed so that the costs of contingency planning do not exceed the costs associated with the risks that the plan is intended to reduce. The plan should also be detailed enough so that its success does not depend on the knowledge or expertise of one or two individuals. It should identify and provide information on

- supporting resources that will be needed;
- roles and responsibilities of those who will be involved in recovery activities;
- arrangements for an off-site disaster recovery location and travel and lodging for necessary personnel, if needed;
- off-site storage location for backup files; and
- procedures for restoring critical applications and their order in the restoration process. (See section CP-1.3 for additional information on emergency processing priorities.)

Multiple copies of the contingency plan should be available, with some stored at off-site locations to make sure they are not destroyed by the same events that made the primary data processing facilities unavailable.

CP-3.2. Arrangements have been made for alternate data processing, storage, and telecommunications facilities

Depending on the degree of service continuity needed, choices for alternative facilities will range from an equipped site ready for immediate backup service, referred to as a “hot site,” to an unequipped site that will take some time to prepare for operations, referred to as a “cold site.” In addition, various types of services can be prearranged with vendors. These include making arrangements with suppliers of computer hardware and telecommunications services as well as with suppliers of business forms and other office supplies.

Exposure Draft

As with all emergency preparations, costs and risks should be considered in deciding what type of alternate site is needed. However, it should be geographically removed from the original site so that it is protected from the same events. In addition, the site should have ready access to the basic utilities needed to resume operations, such as electricity, water, and telecommunications services. In some cases, two or more entities may share the same alternate site in order to reduce the cost. However, this may cause problems if two or more entities need the site at the same time.

Whatever options are determined to be the most appropriate, the entity should have a formal agreement or contract detailing the emergency arrangements. Further, the arrangements should be periodically reviewed to determine whether they remain adequate to meet the agency's needs.

<p><u>CP-3 Related NIST SP-800-53 Controls</u> CP-2 Contingency Plan CP-5 Contingency Plan Update CP-8 Telecommunications Services</p>
--

Exposure Draft

Control Techniques and Suggested Audit Procedures for Critical Element CP-3

Table 36. Control Techniques and Suggested Audit Procedures for Critical Element CP-3: Develop and document a comprehensive contingency plan

Control activities	Control techniques	Audit procedures
CP-3.1. An up-to-date contingency plan is documented.	<p>CP-3.1.1. A contingency plan has been documented that</p> <ul style="list-style-type: none"> • is based on clearly defined contingency planning policy; • reflects current conditions, including system interdependencies; • has been approved by key affected groups, including senior management, information security and data center management, and program managers; • clearly assigns responsibilities for recovery; • includes detailed instructions for restoring operations (both operating system and critical applications); • identifies the alternate processing facility and the back up storage facility; • includes procedures to follow when the data/service center is unable to receive or transmit data; • identifies critical data files; • is detailed enough to be understood by all entity managers; • includes computer and telecommunications hardware compatible with the agency's needs; • includes necessary contact numbers; • includes appropriate system-recovery instructions; • has been distributed to all appropriate personnel; and • has been coordinated with related plans and activities. 	<p>Review contingency planning policy and determine if it documents the agency's overall contingency objectives and establishes the organizational framework and responsibilities for contingency planning.</p> <p>Obtain contingency plans (see NIST SP 800-34) and compare their provisions with the most recent risk assessment and with a current description of automated operations.</p> <p>Compare the contingency plans to security-related plans, facility-level plans, and agency/entity-level plans such as those in NIST contingency planning guidance.</p> <p>Determine if the contingency plans include</p> <ul style="list-style-type: none"> • appropriate consideration of the technology, including alternative processing requirements, • recovery of the security infrastructure, and • interdependencies with other systems (i.e., other component, federal, state, or local agencies) that could affect the contingency operations.
	<p>CP-3.1.2. Contingency plans are reevaluated before proposed changes to the information system are approved to determine if major modifications have security ramifications that require operational changes in order to maintain adequate risk mitigation.</p>	<p>Interview senior management, information security management, and program managers.</p>
	<p>CP-3.1.3. Procedures allow facility access in support of restoration of lost information under the contingency plans in the event of an emergency.</p>	<p>Determine whether emergency and temporary access authorizations are properly approved, documented, controlled, communicated, and automatically terminated after a predetermined period. These procedures should be performed in conjunction with Section AC-3.1.8 and AC-6.1.8 regarding access controls.</p>
	<p>CP-3.1.4. The plan provides for backup personnel so that it can be implemented independent of specific individuals.</p>	<p>Review the contingency plan.</p>
	<p>CP-3.1.5. User departments have developed adequate manual/peripheral processing procedures for use until operations are restored.</p>	<p>Interview senior management, information security management, and program managers.</p>
	<p>CP-3.1.6. Several copies of the current contingency plan are securely stored off-site at different locations.</p>	<p>Observe copies of the contingency and related plans held off-site.</p>

Exposure Draft

Control activities	Control techniques	Audit procedures
	CP-3.1.7. The contingency plan is periodically reassessed and revised as appropriate. At a minimum, the plan is reassessed when there are significant changes in entity mission, organization, business processes, and IT infrastructure (e.g. hardware, software, personnel).	Review the plan and any documentation supporting recent plan reassessments.
CP-3.2. Arrangements have been made for alternate data processing, storage, and telecommunications facilities.	CP-3.2.1. Contracts or interagency agreements have been established for backup processing facilities that <ul style="list-style-type: none"> are in a state of readiness commensurate with the risks of interrupted operations, have sufficient processing and storage capacity, and are likely to be available for use. 	Interview officials and review contracts and agreements including processing priorities for the backup site. Determine if the back up site is properly configured and ready to be used as an operational site.
	CP-3.2.2. Alternate network and telecommunication services have been arranged.	Interview officials and review contracts and agreements including the priority of service provisions for the backup service provider. Determine if the backup service provides separate failure points and is geographically removed from the primary provider.
	CP-3.2.3. Arrangements are planned for travel, lodging, and protection of necessary personnel, if needed.	Interview officials and review the plan.

Source: GAO.

Critical Element CP-4. Periodically test the contingency plan and adjust it as appropriate

Testing contingency plans is essential to determining whether they will function as intended in an emergency situation. According to OMB, federal managers have reported that testing revealed important weaknesses in their plans, such as backup facilities that could not adequately replicate critical operations as anticipated. Through the testing process, these plans were substantially improved.⁸⁸

The most useful scenarios involve simulating a disaster situation to test overall service continuity. Such an event would include testing whether the alternative data processing site will function as intended and whether critical computer data and programs

⁸⁸Observations of Agency Computer Security Practices and Implementation of OMB Bulletin No.90-08: Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information, February 1993. OMB Bulletin 90-08 was superseded by NIST Special Publication (SP) 800-18, dated December 1998, *Guide for Developing Security Plans for Information Technology Systems*. [OMB Circular A-130, Appendix III, directs NIST to update and expand security planning guidance.]

Exposure Draft

recovered from off-site storage are accessible and current. In executing the plan, managers will be able to identify weaknesses and make changes accordingly. Moreover, tests will assess how well employees have been trained to carry out their roles and responsibilities in a disaster situation.

CP-4.1. The plan is periodically tested

The frequency of contingency plan testing will vary depending on the criticality of the agency's operations. Generally, contingency plans for very critical functions should be fully tested about once every year or two, whenever significant changes to the plan have been made, or when significant turnover of key people has occurred. It is important for top management to assess the risks of contingency plan problems and develop and document a policy on the frequency and extent of such testing.

CP-4.2. Test results are analyzed and the contingency plan is adjusted accordingly

Contingency test results provide an important measure of the feasibility of the contingency plan. As such, they should be reported to top management so that the need for modification and additional testing can be determined and so that top management is aware of the risks of continuing operations with an inadequate contingency plan.

Any testing of contingency plans is likely to identify weaknesses in the plan, and it is important that the plan and related supporting activities, such as training, be revised to address these weaknesses. Otherwise, the benefits of the testing will be mostly lost.

Control Techniques and Suggested Audit Procedures for Critical Element CP-4

<p>CP-4 Related NIST SP-800-53 Controls CP-4 Contingency Plan Testing and Exercises CP-5 Contingency Plan Update</p>
--

Exposure Draft

Table 37. Control Techniques and Suggested Audit Procedures for Critical Element CP-4: Periodically test the contingency plan and adjust it as appropriate

Control activities	Control techniques	Audit procedures
CP-4.1. The plan is periodically tested.	CP-4.1.1. The contingency plan is periodically tested under conditions that simulate a disaster. Disaster scenarios tested may be rotated periodically. Typically, contingency plans are tested annually or as soon as possible after a significant change to the environment that would alter the assessed risk.	Review testing policies and methodology used to select disaster scenarios. Determine when and how often contingency plans are tested. Determine if technology is appropriately considered in periodic tests of the contingency plan and resulting adjustments to the plan. Review test results. Observe a disaster recovery test.
CP-4.2. Test results are analyzed and the contingency plan is adjusted accordingly.	CP-4.2.1. Test results are documented and a report, such as a lessons learned report, is developed and provided to senior management.	Review final test report. Interview senior managers to determine if they are aware of the test results.
	CP-4.2.2. The contingency plan and related agreements and preparations are adjusted to correct any deficiencies identified during testing.	Review any documentation supporting contingency plan adjustments.

Source: GAO.

Exposure Draft

Chapter 4. Evaluating and Testing Business Process Application Controls

4.0 Overview

Business processes are the principal functions used by the entity to accomplish its mission. Examples of typical business processes in government entities include:

- Mission-related processes, typically at the program or sub-program level, such as education, public health, law enforcement, or income security;
- Financial management processes, such as collections, disbursements, or payroll; and
- Other support processes, such as human resources, or property management, and security.

A business process application is a combination of hardware and software that is used to process business information in support of a specific business process.

Business process application level controls, commonly referred to as “application level controls” or “application controls”, are those controls over the completeness, accuracy, validity and confidentiality of transactions and data during application processing. The effectiveness of application level controls is dependent on the effectiveness of entitywide and system level general controls. Weaknesses in entitywide and system level general controls can result in unauthorized changes to business process applications and data that can circumvent or impair the effectiveness of application level controls.

If entitywide and system level controls are relevant to the audit objectives, the auditor should coordinate the planning and testing of such controls with application level controls. For example, if a data management system is a critical control point, the auditor would

Exposure Draft

coordinate the planning of testing of the entitywide, system, and application level controls associated with the data management system.

In this chapter, application level controls are divided into the following four control categories, which are described in more detail below:

- (1) Application level general controls;
- (2) Business Process controls;
- (3) Interface controls; and
- (4) Data Management System controls.

The auditor should assess the effectiveness of controls in each of the four control categories to the extent they are significant to the audit objectives.

Application level general controls (referred to herein as “application security” or AS) consist of general controls operating at the business process application level, including those related to security management, access controls, configuration management, segregation of duties, and contingency planning. In this chapter, the general control activities discussed in Chapter 3, as well as related suggested control techniques and audit procedures, are tailored to the business process application level.

Business Process (BP) controls are the automated and/or manual controls applied to business transaction flows. They relate to the completeness, accuracy, validity and confidentiality of transactions and data during application processing. They typically cover the structure, policies, and procedures that operate at a detailed business process (cycle or transaction) level and operate over individual transactions or activities across business processes. Specific control areas of business process controls are:

- **Transaction Data Input** relates to controls over data that enter the application (e.g., data validation and edit checks).

Exposure Draft

- **Transaction Data Processing** relates to controls over data integrity within the application (e.g., review of transaction processing logs).
- **Transaction Data Output** relates to controls over data output and distribution (e.g., output reconciliation and review).
- **Master Data Setup and Maintenance** relates to controls over master data, the key information that is relatively constant and shared between multiple functions or applications (e.g., vendor file).

Interface controls (IN) consist of those controls over the a) timely, accurate, and complete processing of information between applications and other feeder and receiving systems on an on-going basis, and b) complete and accurate migration of clean data during conversion.

Data management system (DA) controls are relevant to most business process applications because applications frequently utilize the features of a data management system to enter, store, retrieve or process information, including detailed, sensitive information such as financial transactions, customer names, and social security numbers. Data management systems include database management systems, specialized data transport/communications software (often called middleware), data warehouse software, and data extraction/reporting software. Data management system controls enforce user authentication/authorization, availability of system privileges, data access privileges, application processing hosted within the data management systems, and segregation of duties. Chapter 3 addresses general controls over data management systems as part of system level controls. This chapter discusses their use within the application level.

For each of the four application control categories, this chapter identifies several critical elements--tasks that are essential for establishing adequate controls within the category. For each critical element, there is a discussion of the associated objectives, risks, and control activities, as well as potential control techniques and

Exposure Draft

suggested audit procedures. For each critical element, the auditor should make a summary determination as to the effectiveness of the entity's related controls in achieving the critical element. If the controls for one or more of each category's critical elements are ineffective, then the controls for the entire category are not likely to be effective. The auditor should use professional judgment in making such determinations.

To facilitate the auditors' evaluation, tables identifying commonly used control techniques and related suggested audit procedures are included after the discussion of each critical element. These tables can be used for both the preliminary evaluation and the more detailed evaluation and testing of controls. For the preliminary evaluation, the auditor can use the tables to guide and document preliminary inquiries and observations. For the more detailed evaluation and testing, the auditor can use the suggested audit procedures in developing and carrying out a testing plan. Such a testing plan would include more extensive inquiries; observation of control procedures; inspection of application configurations, design documents, policies and written procedures; and tests of key control techniques, which may include using audit or system software auditing tools.

The discussion of control elements and control techniques apply to all application environments, which include mainframe, client-server, integrated enterprise resource planning (ERP)

⁸⁹ and web environments. The nature of evidence obtained by the auditor will be different based on the environment. Auditors' knowledge of the business processes and application level security in different environments is, therefore, critical to identifying and testing business process application level controls.

As noted earlier, the effectiveness of application level controls is dependent on the effectiveness of entitywide and systemlevel

⁸⁹ An enterprise resource planning (ERP) system is a commercial software package that integrates all the information flowing through the entity. ERP systems contain functional modules (e.g., financial, accounting, human resources, and supply chain and customer information) that are integrated within the core system or interfaced to external systems.

Exposure Draft

general controls. Weaknesses in entitywide and system level general controls can result in unauthorized changes to business process applications and data (confidentiality, integrity, and availability) that can circumvent or impair the effectiveness of business process application controls. More specifically,

- Weaknesses in security management can result in inadequate assessment of and response to information security risks related to the business process applications and the systems on which they depend, as well as significantly increase the risk that application level and other controls are not consistently applied in accordance with management's policies.
- Weaknesses in access controls can result in unauthorized access to and modifications of
 - applications, including the operation of the related controls,
 - application data, including after the control(s) were applied, and/or
 - system components, which can lead to unauthorized changes to data and applications.
- Weaknesses in configuration management can result in unauthorized modifications or additions to the applications and to system components, leading to unauthorized access to data and applications.
- Weaknesses in segregation of duties can result in unauthorized access to applications, application data, and/or system components. In addition, such weaknesses can allow fraudulent transactions and control overrides to occur.
- Weaknesses in contingency planning can result in unavailability of applications and/or loss of application data.

The following table illustrates the relationship between business process application level controls and general controls at the entitywide and system level.

Exposure Draft

Table 38. General and Application Control Categories Applicable at Different Levels of Audit

	Control Categories	Entitywide/ Component Level	System Level			Business Process Application Level
			Network	Operating Systems	Infrastructure Applications	
General Controls	Security Management					
	Access Controls					
	Configuration Management					
	Segregation of Duties					
	Contingency Planning					
Business Process Application Controls	Business Process Controls					
	Interfaces					
	Data Management Systems					

Source: GAO.

Exposure Draft

4.0.1 The Auditor's Consideration of Business Process Control Objectives

The overall objectives of business process application level controls are to provide reasonable assurance about the completeness, accuracy, validity and confidentiality of transactions and data during application processing. Each specific business process control technique is designed to achieve one or more of these objectives. The effectiveness of business process controls depends on whether all of these overall objectives are achieved. Each objective is described in more detail below.

Completeness (C) controls should provide reasonable assurance that all transactions that occurred are input into the system, accepted for processing, processed once and only once by the system, and properly included in output. Completeness controls include the following key elements:

- transactions are completely input,
- valid transactions are accepted by the system,
- duplicate postings are rejected by the system,
- rejected transactions are identified, corrected and re-processed; and
- all transactions accepted by the system are processed completely.

The most common completeness controls in applications are batch totals, sequence checking, matching, duplicate checking, reconciliations, control totals and exception reporting.

Accuracy (A) controls should provide reasonable assurance that transactions are properly recorded, with the correct amount/data, and on a timely basis (in the proper period); key data elements input for transactions are accurate; and data elements are processed accurately by applications that produce reliable results; and output is accurate.

Exposure Draft

Accuracy control techniques include programmed edit checks (e.g., validations, reasonableness checks, dependency checks, existence checks, format checks, mathematical accuracy, range checks, etc.), batch totals and check digit verification.

Validity (V) controls should provide reasonable assurance (1) that all recorded transactions actually occurred (are real), relate to the organization, and were properly approved in accordance with management's authorization; and (2) that output contains only valid data. A transaction is valid when it has been authorized (for example, buying from a particular supplier) and when the master data relating to that transaction is reliable (for example, the name, bank account and other details on that supplier). Validity includes the concept of authenticity. Examples of validity controls are one-for-one checking and matching.

Confidentiality (CF) controls should provide reasonable assurance that application data and reports and other output are protected against unauthorized access. Examples of confidentiality controls include restricted physical and logical access to sensitive business process applications, data files, transactions, and output, and adequate segregation of duties. Confidentiality also includes restricted access to data reporting/extraction tools as well as copies or extractions of data files.

The completeness, accuracy, and validity controls relate to the overall integrity objective. The availability objective is addressed as part of application level general controls in AS-5.

4.0.2 Steps in Assessing Business Process Application Level Controls

The assessment of business process application level controls is incorporated into the audit approach discussed in Chapter 2. This section provides supplemental implementation guidance with respect to planning the assessment of business process application level controls and should be applied in conjunction with Chapter 2. Consistent with Chapter 2, the assessment of business process application level controls includes the following steps:

- Plan the information system controls audit

Exposure Draft

- Perform information system controls audit tests
 - Report audit results
-

4.0.3 Plan the Information System Controls Audit of Business Process Application Level Controls

Although planning continues throughout the audit, the objectives of the initial planning phase are to identify significant issues, assess risk, and design efficient and effective audit procedures. To accomplish this, the auditor performs the following steps, which are discussed in more detail in Chapter 2:

- Understand the overall audit objectives and related scope of the business process application control assessment
- Understand the entity's operations and key business processes
- Obtain a general understanding of the structure of the entity's networks
- Identify key areas of audit interest (files, applications, systems, locations)
- Assess information system risk on a preliminary basis
- Identify critical control points
- Obtain a preliminary understanding of business process application level controls
- Perform other audit planning procedures

The following discussion provides additional audit considerations for certain of these steps, as they apply to application level controls.

4.0.3.A Understand the overall audit objectives and related scope of the business process application control assessment

The auditor should obtain an understanding of the objectives of the application control assessment. The nature, timing and extent of the

Exposure Draft

auditor's procedures to assess the effectiveness of application controls vary depending upon the audit objectives.

The audit objectives for an application control assessment could include:

- Assessment as part of a broad assessment of information system controls (including entitywide, system, and application level controls), either as part of a financial statement or performance audit, or as a standalone assessment;
- A comprehensive assessment of application level controls related to a specific application or applications, with or without an assessment of related entitywide and system level controls;
- An assessment of specific aspects of application level controls, such as:
 - a. Evaluating the efficiency of business process applications;
 - b. Assessing business process application level controls for applications under development;
 - c. Assessing selected business application level control categories, such as business process controls or application level general controls;
 - d. Assessing conversion of data to a new application; or
 - e. Assessing access controls to assess whether access granted is appropriately identified, evaluated, and approved.

As noted in Chapter 2, if achieving the audit objectives does not require an overall conclusion on IS controls or relates only to certain components or a subset of controls, the auditor's assessment would not necessarily identify all significant IS control weaknesses that may exist. Consequently, if the audit objectives only relate to a subset of controls, such as only business process controls for a specific application, the auditor should evaluate the potential limitations of the auditor's work on the auditor's report and the needs and expectations of users. The auditor may determine that, because the limitations are so significant, the auditor will (1) communicate the limitations to the management of the audited entity, those charged with governance, and/or those requesting the

Exposure Draft

audit, and (2) clearly report such limitations on the conclusions in the audit report. For example, in reporting on an audit limited to business process controls within a business process application, the auditor may determine that it is appropriate to clearly report that the scope of the assessment was limited to those business process controls and that, consequently, additional information system control weaknesses may exist that could impact the effectiveness of IS controls related to the application and to the entity as a whole.

4.0.3.B Understand the entity's operations and key business processes

Understanding the entity's operations and business processes includes understanding how business process applications are used to support key business processes, as it tends to vary from entity to entity. The auditor should obtain and review documentation, such as design documents, blueprints, business process procedures, user manuals, etc., and inquire of knowledgeable personnel to obtain a general understanding of each significant business process application that is relevant to the audit objectives. This includes a detailed understanding of

- business rules (e.g. removing all transactions that fail edits or only selected ones based on established criteria),
- transaction flows (detailed study of the entity's internal controls over a particular category of events that identifies all key procedures and controls relating to the processing of transactions), and
- application and software module interaction (transactions leave one system for processing by another, e.g. payroll time card interfaces with pay rate file to determine salary information).

Obtaining this understanding is essential to assessing information system risk, understanding application controls, and developing relevant audit procedures.

The concept of materiality/significance, discussed in Chapter 2, can help the auditor determine which applications are significant, or key, to the audit objectives.

Exposure Draft

4.0.3.C Obtain a general understanding of the structure of the entity's networks

The auditor should obtain an understanding of the specific networks and systems that are used to support the key business process applications. Information obtained during this step is important to

- (1) Assist in the identification of the critical control points (see Chapter 2) over which entitywide and system level controls need to be effective for the related application level controls to be effective. Based on the results of audit procedures, the auditor may modify the listing of critical control points, or identify additional critical control points. In the testing phase, the auditor assesses entitywide and system level controls (as outlined in Chapter 3) over each critical control point identified, unless not part of the objectives of the audit.
- (2) Provide a foundation for understanding where application level general controls are applied. For example, application level general controls may be applied as part of the application itself, through access control software, data management systems, ERP systems, and/or in conjunction with operating system and network security. Obtaining such an understanding is important to identify those controls that are necessary to reasonably assure that unauthorized access to key applications and data files are prevented or detected.

4.0.3.D Identify key areas of audit interest (files, applications, systems, locations)

Based on the audit objectives and the auditor's understanding of the business processes and networks, the auditor should identify key areas of audit interest, including:

- key business process applications and where each key business process application is processed,
- key data files used by each key business application, and
- relevant general controls at the entitywide and system levels, upon which application level controls depend.

Chapter 2 provides additional information on identifying key areas of audit interest.

Exposure Draft

4.0.3.E Assess information system risk on a preliminary basis

Based on the auditor's understanding obtained in the previous steps, the auditor should assess, on a preliminary basis, the nature and extent of IS risk related to the key applications. The auditor may classify security risks according to the definitions explained in Chapter 2.

Chapter 2 provides a description of risk factors that are relevant to an assessment of IS risk, including nature of the hardware and software used, the configuration of the network, and the entity's IT strategy. The auditor should evaluate such risk factors in relation to the specific key business process applications. For example, Internet accessible applications, and applications that provide access to assets, such as payment or inventory systems, generally present a higher degree of risk.

4.0.3.F Identify critical control points

As discussed in Chapter 2, the auditor should identify and document critical control points in the entity's information systems and key applications, based on the auditor's understanding of such systems and applications, key areas of audit interest, and IS risk. Based on information obtained during audit planning, the auditor identifies critical control points related to the entity's key applications (applications that are significant to the audit objectives and key areas of audit interest). Critical control points at the application level (in addition to critical control points at the system levels) are those points, which if compromised, could significantly affect the integrity, confidentiality, or availability of key business process applications or related data. Critical control points at the business process application level typically include application level general controls, and interface controls among several applications. Typical critical control points also include network components where business process application level controls are applied. As the audit testing proceeds and the auditor gains a better understanding of the applications, application functionality, controls within and outside each application, control weaknesses, and related risks, the auditor should reassess and reconsider the critical control points.

Exposure Draft

4.0.3.G Obtain a preliminary understanding of application controls

Within each key business process application, the auditor should obtain an understanding of the particular types of application level controls that are significant to the audit objectives. If the audit objectives relate to a comprehensive assessment of the effectiveness of application controls within one or more applications, the auditor should obtain an understanding of controls implemented by the entity to achieve each of the critical elements for each key application. If the assessment of application controls is performed in connection with a financial audit, the auditor should assess the effectiveness of those controls that are identified by the financial auditor (controls identified in the Specific Control Evaluation (SCE) Worksheet in federal financial audits) and other related controls upon which the effectiveness of these controls depend. The responsibility to identify financial reporting controls rests primarily with the financial auditor, but the information systems auditor should be consulted in this process. Financial reporting controls generally contain both computer-related (those whose effectiveness depends on computer processing) and non-computer-related controls. Computer-related controls include: general controls, application controls, and user controls. The SCE Worksheet is more fully discussed in section 395 H of the Financial Audit Manual (FAM).

The auditor should obtain a preliminary understanding of business process application controls in each of the following control categories to the extent they are significant to the audit objectives:

- Application level general controls;
- Business Process;
- Interface controls; and
- Data management systems.

Frequently each type of control occurs within a business process and such controls are interdependent. The auditor should consider the interaction between each of these types of controls. For example, interface and data management controls are inter linked since many of the feeder systems reside on some type of data management system whose controls must be effective to ensure the integrity of the data it maintains, including social security numbers,

Exposure Draft

vendor names, and other sensitive information. Further, interface and business process controls are linked in that controls should be established that ensure the timely, accurate and complete processing of information between the feeder and receiving systems and the mainline business processes they support.

To document the auditor's understanding, the auditor may complete the control tables in Appendices II and III on a preliminary basis. The auditor generally should review available application documentation that explains processing of data within the application. The auditor generally should inspect any narratives, flowcharts, and documentation related to system and application, including error reporting.

As part of this step, the auditor should determine whether application level controls are effectively designed. In considering whether controls are effectively designed, the auditor considers the type of control. The effectiveness of business process application controls, and the nature, timing, and extent of assessment procedures, depend on the nature of the control.

As discussed in Chapter 1, information system (IS) controls consist of those internal controls that are dependent on information systems processing and include general controls (entitywide, system, and business process application levels), business process application controls (input, processing, output, master file, interface, and data management system controls), and user controls (controls performed by people interacting with information systems). General and business process application controls are always IS controls. A user control is an IS control if its effectiveness depends on information systems processing or the reliability (accuracy, completeness, and validity) of information processed by information systems. Conversely, a user control is not an IS control if its effectiveness does not depend on information systems processing or the reliability of information processed by information systems.

Application controls can be automated or manual. The auditor will find that most business processes will have a combination of automated and manual controls that balance resource requirements

Exposure Draft

and risk mitigation. Also, management may use manual controls as effective monitoring controls. It is important to understand how these types of controls inter-relate when assessing application controls. The auditor should evaluate the adequacy of controls, both automated and manual, to determine whether or not management has appropriately mitigated risks and achieved its control objectives.

Automated business process controls can provide a higher level of consistency in application, and can also be timelier in preventing an undesired outcome. Automated controls have greater consistency because once designed and implemented, they will continue to operate as designed, assuming the presence of effective general controls (at all levels). Automated controls can also be designed to block a transaction from proceeding through the process, making them timelier in preventing an undesired outcome. For example, a vendor invoice can be blocked for payment automatically if the goods or services are not received or if the payment exceeds a specific threshold and requires additional review and approval. Manual controls, such as the review of reports or payments over a certain amount, could effectively detect an invoice payment without goods receipt, or a high-dollar payment, but may not occur in time to stop the payment.

The operating effectiveness of an automated application control during the audit period also depends on the operating effectiveness of related general controls (at the entitywide, system and applications levels). For example, effective general controls are necessary to prevent or detect management overrides or other unauthorized changes to computer applications or data that could preclude or impair the operation of the automated control.

Automated controls can be further subdivided into

- **Inherent Controls** are those that have been hard coded and built into the application logic and cannot be changed by end users. The self-balancing capability provided by some applications is an example of an inherent control (e.g., in a financial application, the transaction will not post until debits = credits).

Exposure Draft

- **Configurable Controls** are those that have been designed into the system during application implementation and address the features most commonly associated with options available to guide end users through their assigned tasks. Workflow to approve purchase requisition and purchase orders, commitments not to exceed obligations, and dollar value threshold to process transactions are examples of configurable controls.

ERP systems by design are Extensible Business Reporting Language (XBRL) compliant, which means that they can be configured to prepare reports based upon standard rules or “taxonomies.” The auditor should understand the nature and extent of any XBRL use and evaluate the controls surrounding such reporting processes.

Automated controls cannot contemplate and reasonably forecast the outcome of every type of uncertainty, nor can it prevent or detect every possible error or intentional misuse of application functionality. For example, well-designed segregation of duty controls could be compromised by collusion. Manual controls, therefore, may be used either in situations where ideal controls, such as complete segregation of duties, can't be implemented to prevent something from occurring, or when manual controls offer an effective, cost-effective control option.

Manual controls (sometimes referred to as user controls) require human involvement, usually by way of approval of a critical step in a business process (example: signed purchase requisition) or reviewing for exceptions and compliance by reviewing system output. Generally, the auditor considers and tests manual controls along with automated controls. Testing only one type of application control may lead to incorrect assessment of key controls management may be relying on.

When the effectiveness of a manual control that is significant to the audit objectives depends on the reliability of computer-processed information, it is considered an IS control and, the auditor should assess the effectiveness of relevant general (at the entitywide, system, and application levels) and business process application, controls over the reliability of the information used. Also, the

Exposure Draft

effectiveness of manual controls is dependent on how consistently and effectively the control is applied. The auditor considers the following when reviewing manual controls:

- The competence of the individuals performing control activities (reviewing the reports or other documents). They should have an adequate level of business knowledge and technical expertise and be familiar with the entity's operations.
- The authority of the individuals performing the reviews to take corrective action. They should be adequately positioned within the entity to act effectively.
- The objectivity of the individuals performing the reviews. The individuals should be independent of those who perform the work, both functionally (that is, there should be adequate segregation of duties) and motivationally (for example, a review would be less effective if the reviewer's compensation is based on operating results being reviewed).
- The nature and quality of the information reviewed by management.
- The frequency and timeliness of performance of reviews.
- The extent of follow-up performed by management.
- The extent to which controls can be tested (i.e., the auditor's ability to corroborate management's responses to inquiries).

In addition to automated and manual controls performed prior to or during transaction processing, monitoring controls may be applied by management after the processing has taken place. Their objective is to identify any errors that have not been prevented or detected by other controls. Examples of monitoring controls include:

- Review of a report of revenue with overall knowledge of the volume of goods shipped.
- Monitoring of capital expenditures via a quarterly report that analyzes expenditures by department with comparisons to budgeted levels.
- Monitoring of budget versus actual program cost.

Exposure Draft

4.0.3.H Perform other audit planning procedures

As discussed in more detail in Chapter 2, the auditor should address the following issues during the planning phase that could affect the application control audit:

- relevant laws and regulations
- staffing and other resources needed to perform the audit
- multi-year planning
- communication to management officials concerning the planning and performance of the audit, and to others as applicable;
- use of service organizations;
- using the work of others; and
- preparation of an audit plan.

4.0.4 Perform Information System Controls Audit Tests of Business Process Application Level Controls

The auditor's assessment of application controls has two main aspects: testing the effectiveness of controls, and evaluating the results of testing. The process of testing and evaluation are planned and scoped during the planning phase, as discussed in Chapter 2. As the auditor obtains additional information during control testing, the auditor should periodically reassess the audit plan and consider whether changes are appropriate.

The auditor should perform the following procedures as part of testing and evaluating the effectiveness of application level controls:

- Understand information systems relevant to the audit objectives, building on identification of key areas of audit interest and critical control points.
- Determine which IS control techniques are relevant to the audit objectives. The control categories, critical elements, and control activities in Chapters 3 and 4 are generally relevant to all audits. However, if the auditor is not performing a comprehensive audit, for example, an application review, then there may be no need to assess controls in Chapter 3.
- For each relevant IS control technique, determine whether it is suitably designed to achieve the critical activity and has been implemented – placed in operation (if not done earlier);

Exposure Draft

- Perform tests to determine whether such control techniques are operating effectively;
- Identify potential weaknesses in IS controls (weaknesses in design or operating effectiveness); and
- For each potential weakness, consider the impact of compensating controls or other factors that mitigate or reduce the risks related to the potential weakness.

The auditor considers the following in designing the tests of application level controls:

- The nature of the control;
- The significance of the control in achieving the control objective(s);
- The risk of the control not being properly applied. [also see FAM 340];
- All of the key controls that management is relying on to address the risks for a specific business process or a sub-process, which may include automated and manual controls;
- The key controls outside the application under audit, as the business process may involve other applications for a downstream or upstream sub-process; and
- The strength or weakness of the entitywide and system level controls. The depth of the testing is based on the level of risk of the entity under review and the audit objectives. In the absence of effective general controls, the auditor may conclude that business process application level controls are not likely to be effective.

4.0.5 Report Audit Results

As a final step of the audit of application level controls, the auditor should conclude on the individual aggregate effect of identified application control weaknesses on the audit objectives and report the results of the audit. Such conclusions generally should include the effect of any weaknesses on the entity's ability to achieve each of the critical elements in Chapters 3 and 4, and on the risk of unauthorized access to key systems or files. The auditor's conclusions should be based upon the potential interdependencies

Exposure Draft

of application controls (i.e., controls which effectiveness depends on the effectiveness of other controls).

Prior to developing an audit report, it is generally appropriate to communicate identified weaknesses to management to obtain their concurrence with the facts and to understand whether there are additional factors that are relevant to the auditor's evaluation of the effect of the weaknesses. Communication of identified weaknesses to management typically includes the following information:

- Nature and extent of risks
- Control Objectives
- Control Activity
- Findings (including condition, criteria, and where possible, cause and effect), and
- Recommendations

Chapter 2 provides additional guidance on reporting audit results.

Exposure Draft

4.1. Application Level General Controls (AS)

Application level general controls consist of general controls operating at the business process application level, including those related to security management, access controls, configuration management, segregation of duties, and contingency planning. In this chapter, the general control activities discussed in Chapter 3, as well as related suggested control techniques and audit procedures, are tailored to the application level. Understanding business processes or events is necessary to determine the role of application level general controls in the assessment of business process application controls.

Chapter 3 addresses controls at the entitywide and system levels, such as those related to networks, servers, general support systems and databases that support one or more business and financial systems. Additional security considerations specific to applications are discussed in this section.

Application level general controls are dependent on general controls operating at the entitywide and system levels. The application is generally a subset of the infrastructure that includes one or more operating systems, networks, portals, LDAPs, and data management systems. For example, the system level access controls discussed in Chapter 3 apply to the users of the application. In addition, applications themselves require another level of access requirements that restrict users to application functionality that aligns with the user's role in the organization. The objective of application level general controls is to help entity management assure the confidentiality, integrity, and availability of information assets, and provide reasonable assurance that application resources and data are protected against unauthorized:

- Modification,
- Disclosure,
- Loss, and
- Impairment

Exposure Draft

Weaknesses in application level general controls can result in unauthorized access, use, disclosure, disruption, modification, or destruction of applications and application data. Consequently, weaknesses in application level general controls can affect the achievement of all of the control objectives (completeness, accuracy, validity, and confidentiality) related to applications data. Therefore, the control activities in the control tables for application level general controls do not contain reference to specific control objectives.

The evaluation of application level general controls is comprised of critical elements in the following areas: Security Management, Access Control, Configuration Management, Segregation of Duties and Contingency Planning. Application-specific technical knowledge is essential to assess the application level general controls.

The critical elements for application level general controls are:

- AS-1 - Implement effective application security management
- AS-2 - Implement effective application access controls
- AS-3 - Implement effective application configuration management
- AS-4 - Segregate application user access to conflicting transactions and activities and monitor segregation
- AS-5 - Implement effective application contingency planning

The related NIST SP 800-53 controls are identified in Chapter 3.

Critical Element AS-1. Implement effective application security management.

Effective application security management provides a foundation for entity management to obtain reasonable assurance that the application is effectively secure. Application security management provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's application-related controls. Without effective security management over the application, there is an increased risk that entity management, IT staff, and application owners and users will not properly assess risk and will, consequently, implement inappropriate and/or inadequate information security over the

Exposure Draft

application. Consistent with security management at the entitywide and system levels, application security management includes the following key components, which are discussed in more detail below:

- Establish an application security plan
- Periodically assess and validate application security risks
- Document and implement application security policies and procedures
- Ensure that application owners and users are aware of application security policies and procedures
- Monitor the effectiveness of the security program
- Effectively remediate information security weaknesses
- Implement effective security-related personnel policies
- Adequately secure, document and monitor external third party activities

Establish an application security plan

An application security plan serves as a roadmap during the entire security development and maintenance lifecycle of the application, and is therefore critical to the auditor in gaining a high-level understanding of the entity's application security. The lack of a comprehensive, documented security design increases the risk of inappropriate system access and compromised data confidentiality, integrity, and availability. Risks of not having a security program at the application level include the following:

- The process to gather design requirements may be compromised without clear guidelines on approval and sign off procedures for security roles.
- Ongoing requirements for business process owners to provide authorization specifications to the security design team (e.g., field-level security, role testing, etc.) may be compromised without a guideline to drive the joint-effort process.
- Security roles could be defined inappropriately resulting in users being granted excessive or unauthorized access.

For federal systems, NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*,

Exposure Draft

provides guidance on documenting information system security controls. The general guidance in SP 800-18 is augmented by SP 800-53 with recommendations for information and rationale to be included in the system security plan.

Periodically assess and validate application security risks

Chapter 3 (SM-2) discusses comprehensive risk assessment, and provides guidance on risk assessment. The guidance includes requirements contained in various regulatory requirements, such as FISMA, FMFIA and OMB Circular A-130, and standards developed by NIST⁹⁰. Risk assessments should consider risks to data confidentiality, integrity, and availability, and the range of risks that an entity's systems and data may be subject to, including those posed by internal and external users. The Security Management section of Chapter 3 addresses the entitywide and system level security risk assessments. Risk assessments also should be conducted for applications, and documented in the security plan, as discussed in NIST SP 800-18.

Document and implement application security policies and procedures

Based on the application security plan, the entity should document and implement specific policies and procedures that govern the operation of application controls. Policies and procedures should address all business process application level controls, be documented and reflect current application configurations.

In defining policies and procedures for application controls, the following should also be considered:

- High risk business processes – Procurement, Asset Management, Treasury, etc.
- Functionality that should not be widely distributed - For example, limiting vendor master data maintenance to a few users is critical to ensure master data integrity and reliable transaction processing.

⁹⁰ In addition, agency-specific requirements should be addressed.

Exposure Draft

- Segregating master data and transactional data (Contrary to master data, transactional data result from a single event, and often use several field values of the master data.) – For example, combining vendor creation and payment authorization could result in payments to unauthorized vendors.
- Cross-business unit access - Should be limited to users who have a specific business need.

Implement effective security awareness and other security-related personnel policies

It is important that application owners and users are aware of and understand the application security policies and procedures so that they may be properly implemented. Improper implementation could result in ineffective controls and increased information security risks. Awareness programs should be coordinated with the entitywide training program to reasonably assure that the training is appropriate and consistent for all applications.

Monitor the effectiveness of the security program

Policies and procedures for monitoring application security should be integrated with monitoring performed as part of the entitywide information security program. Changes related to people, processes, and technology, often make policies and procedures inadequate. Periodic management evaluation not only identifies the need to change the policies and procedures, when appropriate, but also demonstrates management's commitment to an application security plan that is appropriate to the agency's mission. The basic components of an effective monitoring program are discussed in Chapter 3 (Critical element SM-5), which provides guidelines for monitoring the policies and procedures relevant to application security. Management should have an adequate plan for monitoring policy effectiveness, and should test and document application security controls on a regular basis.

Management should consider ways to effectively coordinate monitoring efforts with work performed to comply with applicable laws and regulations and should consider them in developing an application security monitoring assessment plan. Examples of such

Exposure Draft

requirements for federal entities include: FISMA, OMB Circular A-130 and OMB Circular A-123. FISMA requires that security of all major systems is tested by management annually, which would include applications. The depth and breadth of the testing may vary based on the following factors:

- The potential risk and magnitude of harm to the application or data;
- The criticality of the application to the agency's mission;
- The relative comprehensiveness of the prior year's review; and
- The adequacy and successful implementation of corrective actions for weaknesses identified in previous assessments.

OMB Circular A-130 requires that Federal agencies assess and test the security of major applications at least once every 3 years, as part of the certification and accreditation (C&A) process; sooner if significant modifications have occurred or where the risk and magnitude of harm are high.

OMB Circular A-123 requires agencies and individual Federal managers to take systematic and proactive measures to (i) develop and implement appropriate, cost-effective internal control for results-oriented management; (ii) assess the adequacy of internal control in Federal programs and operations; (iii) separately assess and document internal control over financial reporting consistent with the process defined in Appendix A; (iv) identify needed improvements; (v) take corresponding corrective action; and (vi) report annually on internal control through management assurance statements. The implementation guidance for OMB Circular A-123 includes requirements that are wholly consistent with this manual.

The entity should take into consideration the statutory and regulatory requirements in its assessment of the effectiveness of application security policies and procedures, and testing of application security controls.

Management should:

- develop and document the assessment plan of application security policies and procedures;
- test and document application security controls specific to each application; and

Exposure Draft

- ensure that the frequency and scope of testing are commensurate with the criticality of the application to the agency's mission and risk.

Effectively remediate information security weaknesses

Management's commitment to application security is also demonstrated in having an effective mechanism to address weaknesses and deficiencies identified. When weaknesses or deficiencies are identified in application security, management should assess the risk associated with the weakness or deficiency, and develop a corrective action plan (for federal agencies, OMB refers to these as Plans of Actions and Milestones (POAMs)). The action plan should include testing requirements of corrective actions, milestones, monitoring of activities related to the action plan, modification to policies and procedures (if required) and implementation of the corrective action. Such action plans should be coordinated with the entitywide corrective action plan process.

Implement effective security-related personnel policies

Entitywide security-related personnel policies and procedures (see critical element SM-6) should be properly implemented with respect to the application. For example, controls should be in place to reasonably assure that (1) application users are appropriately trained, and (2) risks related to confidentiality, integrity, and availability are considered in approving user access (e.g., security clearances) and in applying personnel policies.

Adequately secure, document, and monitor external third party activities

An agency may allow external third parties access to their systems for various purposes. Chapter 3 discussed policies and procedures regarding the system access granted to third party providers (e.g. service bureaus, contractors, system development, security management), including the requirement to have appropriate controls over outsourced software development. Third party

Exposure Draft

provider access to applications often extends beyond the software development. It is likely that entities have vendors, business partners and contractors not only querying the applications, but also transacting with the agency, using agency applications, or connecting to the agency's applications via their own systems. In addition, public web sites are sometimes used to transact with the agency.

The impact of an external third party provider accessing the agency's applications is directly related to the magnitude of the system or direct access the provider is granted. This is determined by the entity's agreement with the provider. The entity should, however, require the providers to be subject to the same compliance requirements as the agency, and have the ability to monitor such compliance. Appropriate policies and procedures should exist for monitoring third party performance to determine whether activities performed by these external third parties are compliant with the agency's policies, procedures, privacy requirements, agreements or contracts.⁹¹

⁹¹ See GAO, *Information Security: Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk*, (Washington, D.C.: April 2005).

Exposure Draft

Table 39. Control Techniques and Suggested Audit Procedures for Critical Element AS-1: Implement effective application security management

Control activities	Control techniques	Audit procedures
AS-1.1 A comprehensive application security plan is in place.	AS-1.1.1 A comprehensive application security plan has been developed and documented. Topics covered include: <ul style="list-style-type: none">• Application identification and description• Application risk level• Application owner• Person responsible for the security of the application• Application interconnections/information sharing• A description of all of the controls in place or planned, including how the controls are implemented or planned to be implemented and special considerations• Approach and procedures regarding security design and upgrade process• Process for developing security roles• General security administration policies, including ongoing security role maintenance and development• Identification of sensitive transactions in each functional module• Identification of high risk segregation of duty cases• Roles and responsibilities of the security organization supporting the system with consideration to segregation of duties• Security testing procedures• Coordination with entitywide security policies• Procedures for emergency access to the production system, including access to update programs in production, direct updates to the database, and modification of the system change option• System parameter settings, compliant with entitywide agency policies• Access control procedures regarding the use of system delivered critical user IDs	Inspect the application security plan to determine whether it adequately addresses all of the relevant topics.

Exposure Draft

Control activities	Control techniques	Audit procedures
	<p>AS-1.1.2 Sensitive accounts are identified for each business process or sub-process, and appropriate security access privileges are defined and assigned.</p> <hr/> <p>AS-1.1.3 Access privileges are developed to prevent users from executing incompatible transactions within the application via menus or screens.</p>	<p>Review the entity's identification of sensitive transactions for the business process being audited for appropriateness and completeness.</p> <p>Observe and inspect procedures for identifying and assigning sensitive activities.</p> <p>Inspect authorizations for sensitive activities.</p> <hr/> <p>Through inquiry and inspection, determine whether the application security plan includes plans to identify segregation of duty conflicts in each of the business processes under assessment (master data and transaction data; data entry and reconciliation), and addresses controls to mitigate risks of allowing segregation of duty conflicts in a user's role.</p>
<p>AS-1.2 Application security risk assessments and supporting activities are periodically performed</p>	<p>AS-1.2.1 Security risks are assessed for the applications and supporting systems on a periodic basis or whenever applications or supporting systems significantly change.</p> <p>The risk assessments and validation, and related management approvals, are documented and maintained.</p> <p>The risk assessments are appropriately incorporated into the application security plan.</p>	<p>Obtain the most recent security risk assessment for each application under assessment. Inspect the risk assessments to determine if the risk assessments are up-to-date, appropriately documented, approved by management, and supported by testing. Consider compliance with FISMA, OMB, NIST, and other requirements/ guidance and whether technology and business processes are appropriately considered in the risk assessment.</p> <p>Obtain and inspect the relevant application security plan(s) to determine whether the risk assessments are appropriately incorporated into the application security plan.</p>
<p>AS-1.3 Policies and procedures are established to control and periodically assess access to the application.</p>	<p>AS-1.3.1 Business process owners accept risks and approve the policies and procedures.</p> <p>AS-1.3.2 Policies and Procedures are:</p> <ul style="list-style-type: none"> • documented • appropriately consider business process security needs. • appropriately consider segregation of application user activity from the system administrator activity. 	<p>Determine through interview with entity management whether policies and procedures have been established to review access to the application.</p> <p>Review policies and procedures to determine whether they have appropriately considered (1) business security needs and (2) segregation of application user activity from system administrator activity.</p>

Exposure Draft

Control activities	Control techniques	Audit procedures
AS-1.4 Application owners and users are aware of application security policies	AS-1.4.1 The entity has an effective process to communicate application security policies to application owners and users and reasonably assure that they have an appropriate awareness of such policies.	<p>Obtain an understanding of how application owners and users are made aware of application security policies and assess the adequacy of the process.</p> <p>Interview selected application owners and users concerning their awareness of application security policies.</p>
	AS-1.5 Management periodically assesses the appropriateness of application security policies and procedures, and compliance with them.	<p>AS-1.5.1 An application security policy and procedure test plan is developed and documented.</p> <p>AS-1.5.2 Security controls related to each major application are tested at least annually.</p> <p>AS-1.5.3 The frequency and scope of testing is commensurate with the risk and criticality of the application to the agency's mission.</p> <p>AS-1.5.4 Compliance, and a report on the state of compliance, is part of the entity's security program.</p>
AS-1.6 Management effectively remediates information security weaknesses.	AS-1.6.1 Management has a process in place to correct deficiencies.	Inquire of management and inspect security polices and procedures, including assessment and resolution plan.
	AS-1.6.2 Management initiates prompt action to correct deficiencies. Action plans and milestones are documented and complete.	<p>Inspect recent FMFIA/A-123 and POA&M (or equivalent) reports for reasonableness of corrective actions (nature and timing),.</p> <p>Determine whether application security control deficiencies (identified by the audit, by management testing, and by others) are included in the plans of action and milestones (or equivalent). and determine the status of corrective actions</p>
	AS-1.6.3 Deficiencies are analyzed by application (analysis may be extended to downstream, upstream, and other related applications), and appropriate corrective actions are applied.	Evaluate the scope and appropriateness of planned corrective actions through inquiry of management and inspection of evidence.

Exposure Draft

Control activities	Control techniques	Audit procedures
	AS-1.6.4 Corrective actions are tested after they have been implemented and monitored on a continuing basis.	Inspect documentation to determine if implemented corrective actions have been tested and monitored periodically.
AS-1.7 Implement effective security-related personnel policies	AS-1.7.1 Personnel policies related to the application appropriately address security and application owners and users have adequate training and experience.	Review personnel policies for appropriateness and consistency with entitywide policies. Assess the adequacy of training and expertise for application owners and users.
AS-1.8 External third party provider activities are secure, documented, and monitored	AS-1.8.1 Policies and procedures concerning activities of third party providers are developed and include provisions for: <ul style="list-style-type: none"> • Application compliance with agency's security requirements, and • Monitoring of compliance with regulatory requirements 	Inspect policies and procedures pertaining to external parties for the application under assessment. Inspect documentation to determine whether the external third party provider's need to access the application is appropriately defined and documented.
	AS-1.8.2 A process is in place to monitor third party provider compliance to the agency's regulatory requirements	Inquire of management regarding procedures used to monitor third party providers. Inspect external reports (SAS 70) or other documentation supporting the results of compliance monitoring.

Source: GAO.

Critical Element AS-2. Implement effective application access controls

Effective application access controls should be implemented at the application level to provide reasonable assurance that only authorized personnel have access to the application and only for authorized purposes. Without effective application access controls, persons may obtain unauthorized or inappropriate access to applications and application data.

Application access controls include the following:

- Adequately protect information system boundaries.
- Implement effective identification and authentication mechanisms.
- Implement effective authorization controls.
- Adequately protect sensitive system resources.

Exposure Draft

- Implement an effective access audit and monitoring capability.
- Establish adequate physical security controls.

Adequately protect application boundaries

Application boundaries control logical connectivity to and from applications through controlled interfaces (e.g., gateways, routers, firewalls, encryption). In defining the application, the entity creates the boundaries for the application. Once defined, the entity should design appropriate controls over the flow of information across the application boundary. In complex applications, there may be boundaries within the application. The security plan for the application should identify system boundaries and IS controls implemented to protect the security of such boundaries. Application boundaries are more sensitive where the connectivity is to lower risk systems or to systems or users external to the entity.

Implement effective identification and authentication mechanisms

The entity should have application security policies and procedures in place concerning user identification and authentication. Management should have created an environment where all users have their own unique IDs and passwords, or other mechanisms, such as tokens and biometrics to access any part of the information system and applications that allow them to execute functional responsibilities. Identification and authentication policy and management are discussed in Chapter 3, Critical Element AC-2. In addition, it is important to understand the mechanisms used to assign access privileges for applications under assessment. An evaluation of identification and authentication controls includes consideration of the following factors:

- How do the users access the application?
 - a. Are users required to enter user name/ID and password?
 - b. Do all users have an individual and unique ID that would allow the user's activities to be recorded and reviewed?

Exposure Draft

- c. Are users required to enter/use other authenticating information, such as tokens or biometrics?
 - d. Are users required to enter a separate ID and password for each application?
 - e. Does the application require the user to enter a password?
 - f. What are the password parameters (i.e. length, character requirements, etc)?
 - g. How often does the application require the user to change the password?
 - h. Are there any instances of users having multiple IDs and passwords?
 - i. Are there any instances of users sharing IDs or passwords?
- What other IDs and passwords does the user have to enter before accessing the sign-in screen for the application?
 - a. Does the user enter a network ID and password?
 - b. Does the user enter a terminal emulation ID and password?

The knowledge of the application security design and function enables the auditor to assess the effectiveness of the security controls over the other levels of authentication, especially when weaknesses are identified at the application security layer, as those weaknesses may be mitigated by stronger controls at other levels.

Implement effective authorization controls

The following procedures discussed in Chapter 3 are equally applicable at the application level:

- The owner identifies the nature and extent of access that should be available for each user;

Exposure Draft

- The owner approves user access to the application and data;
- Access is permitted at the file, record, or field level; and
- Owners and security managers periodically monitor user access.

Security administration procedures should provide tactical guidance on the day-to-day operations of creating, assigning, monitoring, updating, and revoking end-user access to the application. End-users should be assigned authorizations sufficient, but not excessive, to perform their duties in the application: Access should be limited to individuals with a valid business purpose (least privilege). The users should be granted the level of access by virtue of the position they hold within the organization. This will generally require user to have both:

- Functional access (for example, accounts payable) based on the role from which their position derives; and
- Organizational access (for example, account payable supervisor) based on the specific needs of their position.

Sensitive transactions and segregation of duty conflicts defined by the process and data owners (discussed in AS-1) should be used as a baseline reference by security administration. In an integrated application environment, the importance of comprehensive identification of sensitive transactions and segregation of duty needs and conflicts is heightened, compared with entities having multiple applications for business processes. Entities lose the inherent segregation in integrated applications—since more of the process is performed in the same application, the opportunities for access throughout the process are greater. For example, in an entity with separate purchasing and accounts payable applications, adequate segregation of duties might be accomplished by only allowing access to one of the applications, whereas in an integrated application, these applications may be combined. Transaction-level restricted access, which is critical in integrated applications, may be less critical in non-integrated systems.

However, in an integrated environment, the entire business process cycle may be performed in the same application and a user may

Exposure Draft

have the ability to perform more than one key activity in the cycle. Therefore, restricted access (access to a sensitive business transaction) and segregation of duty conflicts (access to two or more transactions that are sensitive in combination) should be considered carefully.

An integrated application environment also generally means that more business units of the entity are using the same application. Therefore, business unit access restrictions are also necessary. Management should have an adequate understanding of the business processes and determine whether users should have access to more than their individual business unit. For example, a property manager should not have access to change asset records or maintenance schedules for entities other than his/her own.

Sensitive transactions or activities in an application are determined by the nature and use of the data processed by the application. Factors that determine the sensitivity include the mission critical elements of the application, pervasive use of the data or activity, confidentiality and privacy of data, and activities performed or supported by the application.

The key element in assigning access to sensitive transactions or activities to an application user is the alignment of user access to job responsibility. This has a dual purpose: one, the proper alignment ensures that the user has accountability for proper execution of the transactions and accuracy of the related data, and two, the expertise and skills of the user match the business process underlying the transaction or activity. For example journal voucher entry is made by a General Accounting Account Analyst of Finance Department, and not by a Procurement manager.

Adequately protect sensitive application resources

Access to sensitive application resources should be restricted to individuals or processes that have a legitimate need for this access for the purposes of accomplishing a valid business purpose. Sensitive application resources include password files, access authorizations to read or modify applications, and sensitive application functions such as application security administration. The entity should identify and adequately protect sensitive

Exposure Draft

application resources. In some cases, sensitive data may need to be encrypted.

Implement an effective audit and monitoring capability

Audit and monitoring involves the regular collection, review, and analysis of indications of inappropriate or unauthorized access to the application. Automated controls may be used to identify and report such incidents. An understanding of manual control activities surrounding access to the application is important. The following questions can help the auditor gain insight into management's controls:

- Does management maintain and review a current list of authorized users?
- Does management periodically review the user list to ensure that only authorized individuals have access, and that the access provided to each user is appropriate?
- Does management monitor access within the application (i.e. unauthorized access attempts, unusual activity etc.)? Does the application generate reports to identify unauthorized access attempts? Are security logs created and reviewed?
- Is public access (non agency employees) permitted to the application? Is access permitted via the Internet? If so, how is this access controlled?
- Is the application configured to allow for segregation of duties? If so, does the application identify the users who performed activities that were in conflict? Are the transactions/logs reviewed by the business owners?
- Has a procedure been created and placed in operation that requires a complete user recertification on a periodic basis?
- Is the security administration monitored? When suspicious activities are identified, how does management investigate them?

Exposure Draft

Establish adequate physical security controls

Appropriate physical controls, integrated with related entitywide and system level physical security, should be in place to protect resources, where applicable, at the application level. Resources to be protected at the application level include controls over removable media (e.g., tape files), workstations containing sensitive application data, and physical inputs (e.g., check stock) and outputs (e.g., physical checks or other sensitive documents). The entity should identify application resources that are sensitive to physical access and implement adequate physical security over such resources.

Table 40. Control Techniques and Suggested Audit Procedures for Critical Element AS-2: Implement effective application access controls

Control activities	Control techniques	Audit procedures
AS-2.1 Application boundaries are adequately protected.	AS-2.1.1 Application boundaries are identified in security plans. Application boundaries are adequately secure.	Review security plans for proper identification of application boundaries. Evaluate the effectiveness of controls over application boundaries.
AS-2.2 Application users are appropriately identified and authenticated.	AS-2.2 Identification and authentication is unique to each user. All approved users should enter their user ID (unique) and password (or other authentication) to gain access to the application.	Inspect pertinent policies and procedures, and NIST guidance for authenticating user IDs. Through inquiry, observation or inspection, determine the method of user authentication used (password, token, biometrics, etc.). If a password system is used, gain an understanding of the specific information and evaluate its appropriateness, including application security authentication parameters, via inspection of system reports or observation of the system, including appropriate testing. See AC-2 for more information on criteria for evaluating password policies.

Exposure Draft

Control activities	Control techniques	Audit procedures
AS-2.3 Security policies and procedures appropriately address ID and password management.	<p>AS-2.3.1 The agency has formal procedures and processes for granting users access to the application. The agency's IT security policies and procedures contain guidance for:</p> <ul style="list-style-type: none"> • Assigning passwords; • Changing and resetting passwords; and • Handling lost or compromised passwords 	<p>Through inquiry, observation, and inspection, understand and assess procedures used by the agency for application password management:</p> <ul style="list-style-type: none"> • Procedures for initial password assignment, including the password parameters; • Procedures for password changes, including initial password change; • Procedures for handling lost passwords (password resetting); and • Procedures for handling password compromise.
	<p>AS-2.3.2 The application locks the user's account after a pre-determined number of attempts to log-on with an invalid password. The application may automatically reset the user account after a specific time period (an hour or a day), or may require an administrator to reset the account.</p> <p>If the user is away from his/her workspace for a preset amount of time, or the user's session is inactive, the application automatically logs off the user's account.</p>	<p>After obtaining an understanding of the user authentication process, inspect and/or observe the following:</p> <ul style="list-style-type: none"> • Whether access to the application is permitted only after the user enters their user ID and password. • Observe a user executing invalid logins and describe the actions taken. <p>Either 1) inspect system security settings, or 2) observe an idle user workspace to determine whether the application logs the user off after an elapsed period of idle time.</p>
	AS-2.3.3 Each application user has only one user ID.	<p>Through observation and inspection, determine whether each user has one, and only one, user ID to access the application</p>
	AS-2.3.4 Multiple log-ons are controlled and monitored.	<p>Through inquiry, observation or inspection, determine whether the application allows multiple log-ons by the same user. If so, understand and document monitoring procedures that reasonably assure that multiple log-ons are not used to allow application access to an unauthorized user, or to violate effective segregation of duties.</p>
AS-2.4 Access to the application is restricted to authorized users.	AS-2.4.1 Before a user obtains a user account and password for the application, the user's level of access has been authorized by a manager and the application administrator.	<p>Review policies and procedures. From a sample of user accounts determine whether the user level of access was authorized by appropriate entity management.</p>

Exposure Draft

Control activities	Control techniques	Audit procedures
	AS-2.4.2 Owners periodically review access to ensure continued appropriateness.	Interview security administrators and inspect evidence of the effectiveness of periodic review of access by owners.
	AS-2.4.3 Access is limited to individuals with a valid business purpose (least privilege)	<p>Interview owners and inspect documentation, to determine whether appropriate procedures are in place to remove or modify application access, as needed.</p> <p>Through inquiry, observation, and inspection, determine how an unauthorized user is identified, and whether access is removed promptly and how.</p> <p>Based on the sample of users in AS-2.4.1 above, determine whether the user access is appropriate to the business need. If the users did not execute the transaction or activity within the expected time frame, processes should be in place to evaluate the continued need for access, and modify access accordingly.</p>
AS-2.5 Public access is controlled. (Based on an agency's business mission, the agency may allow the public to have access to the application.)	AS-2.5.1 The agency implements a security plan and process for 1) identification and authorization of users; 2) access controls for limited user privileges; 3) use of digital signatures; 4) prohibition of direct access by the public to production data; and 5) compliance with FISMA and NIST requirements	<p>Obtain an understanding of the following controls through inquiry of the application owner, inspection of source documents, and/or observation of the following:</p> <ul style="list-style-type: none"> ● Identification and authentication; ● Access controls for limiting user privileges(read, write, modify, delete); ● Use of digital signatures; ● Prohibition of direct access by the public to live databases and restricted/sensitive records; and <p>Legal considerations (i.e., privacy laws, FISMA, NIST, etc.).</p>
AS-2.6 User access to sensitive transactions or activities is appropriately controlled.	AS-2.6.1 Owners have identified sensitive transactions or activities for the business process.	Inquire of responsible personnel and inspect pertinent policies and procedures covering segregation of application duties

Exposure Draft

Control activities	Control techniques	Audit procedures
	AS-2.6.2 Owners authorize users to have access to sensitive transactions or activities.	Determine whether the process owners have identified a list of sensitive transactions or activities for their area. Inspect the user administration procedures to determine whether they include a requirement for the process owner to approve access to transactions or activities in their area of responsibility. Through inquiry and inspection, determine whether user access is authorized by process owners.
	AS-2.6.3 Security Administrators review application user access authorizations for access to sensitive transactions and discuss any questionable authorizations with owners.	Select a sample of user access request forms or other authorization documents [can use same sample selected in AS-2.4.1 and AS-2.4.3] and inspect them to determine whether the process owners have approved user access to appropriate transactions or activities.
	AS-2.6.4 Owners periodically review access to sensitive transactions and activities to ensure continued appropriateness.	Interview security administrators and inspect user access authorization procedures to determine whether access to sensitive transactions require approval by the process owner.
	Inactive accounts and accounts for terminated individuals are disabled or removed in a timely manner.	Review security software parameters and review system-generated list of inactive logon IDs, and determine why access for these users has not been terminated. Obtain a list of recently terminated employees and, for a selection, determine whether system access was promptly terminated.

Exposure Draft

Control activities	Control techniques	Audit procedures
	<p>AS-2.6.5 Access to sensitive transactions is limited to individuals with a valid business purpose (least privilege)</p>	<p>Interview owners and inspect documentation, to determine whether appropriate procedures are in place to remove or modify application access, as needed.</p> <p>Through inquiry, observations, and inspection, determine how an unauthorized user is identified, and whether access is removed promptly and how.</p> <p>Obtain a list of users with access to identified sensitive transactions for the business process under assessment. Inspect the list to determine whether the number of users having access to sensitive transactions/ activities is appropriate to the business need. If the users did not execute the transaction or activity within the expected time frame, processes should be in place to evaluate the continued need for access, and modify access accordingly.</p>
<p>AS-2.7 Sensitive application resources are adequately protected</p>	<p>AS-2.7.1 The entity identifies sensitive application resources.</p> <p>Access to sensitive application resources is restricted to appropriate users.</p> <p>Sensitive application data is encrypted, where appropriate.</p>	<p>Evaluate the completeness of sensitive application resources identified.</p> <p>Assess the adequacy of IS controls over sensitive application resources.</p>
<p>AS-2.8 An effective access audit and monitoring program is in place, documented, and approved.</p>	<p>AS-2.8.1 Policies and procedures are established to reasonably assure that application security audit and monitoring is effective</p>	<p>Inspect documented policies and procedures for application security administration for each application in scope</p> <p>Determine whether the monitoring program has built-in procedures to identify inappropriate user assignments.</p> <p>Through inquiry and inspection, determine whether monitoring procedures are performed on a regular basis.</p> <p>Determine whether the exceptions are handled appropriately and in a timely manner.</p>

Exposure Draft

Control activities	Control techniques	Audit procedures
AS- 2.9 Application security violations are identified in a timely manner.	AS-2.9.1 Logging and other parameters are appropriately set up to notify of security violations as they occur.	Observe and inspect application logging and other parameters that identify security violations and exceptions. (For example, parameter set up indicates whether or not users can logon to an application more than once)
AS-2.10 Exceptions and violations are properly analyzed and appropriate actions taken.	<p>AS-2.10.1 Reportable exceptions and violations are identified and logged.</p> <p>Exception reports are generated and reviewed by security administration.</p> <p>If an exception occurs, specific action is taken based upon the nature of exception.</p>	<p>Observe and inspect management's monitoring of security violations, such as unauthorized user access.</p> <p>Inspect reports that identify security violations. Through inquiry and inspection, note management's action taken.</p> <p>Inspect reports of authorized segregation of duty conflicts sensitive process access; Assess business level authorization and monitoring, if applicable</p>
AS-2.11 Physical security controls over application resources are adequate	<p>AS-2.11.1 Physical controls are integrated with entitywide and system-level controls.</p> <p>Application resources sensitive to physical access are identified and appropriate physical security is placed over them.</p>	<p>Review the appropriateness of the entity's identification of application resources sensitive to physical access.</p> <p>Assess the adequacy of physical security over sensitive application resources.</p>

Source: GAO.

Critical Element AS-3 – Implement effective application configuration management

Entities need to proactively manage changes to system environments, application functionality and business processes to reasonably assure financial data and process integrity. To do this, entities should restrict and monitor access to program modifications and changes to configurable objects in the production environment. Configuration Management (CM) discusses changes to baseline configuration of applications, using the concepts of identification, control, status reporting and auditing of configuration. Most application configuration changes are managed using a staging process. The staging process allows the entity to develop and unit test changes to an application within the development environment,

Exposure Draft

transport the changes into a Quality Assurance environment for further system and user acceptance testing and, when the tests have been completed and the changes are approved, transport the changes into the production environment.

Control over business process applications modifications and configurable objects is an extension of Configuration Management controls in Chapter 3 that addresses an organization's change management process and should be coordinated with audit procedures applied to that general control category. This chapter includes changes to application functionality that do not go through the staging process, but take place directly in the production environment of the application as changes become necessary throughout the normal course of business.

Effective application configuration management, consistent with Section 3.3 Configuration Management (CM), includes the following steps:

1. Develop and document CM policies, plans, and procedures.
2. Maintain current configuration identification information.
3. Properly authorize, test, approve, and track all configuration changes, including
 - Documented system development life cycle methodology (SDLC);
 - Adequate authorization of change requests that are documented and maintained;
 - Appropriate authorization for the user to change the configuration;
 - Adequate control of program changes through testing to final approval;
 - Adequate control of software libraries; and

Exposure Draft

- Appropriate segregation of duties over the user's access to reasonably assure that critical program function integrity is not affected;

4. Routinely monitor the configuration.

5. Update systems in a timely manner to protect against known vulnerabilities.

6. Appropriately document, test, and approve emergency changes to the configuration.

In addition, NIST SP 800-100 provides guidance in assessing related configuration management programmatic areas of capital planning and investment control, and security services and product acquisition. This publication discusses practices designed to help security management identify funding needs to secure systems and provide strategies for obtaining the necessary funding. Also, it provides guidance to entities in applying risk management principles to assist in the identification and mitigation of risks associated with security services acquisitions.

Table 41. Control Techniques and suggested audit procedures for AS-3 - Implement Effective Application Configuration Management

Control activities	Control techniques	Audit procedures
AS-3.1 Policies and procedures are designed to reasonably assure that changes to application functionality in production are authorized and appropriate, and unauthorized changes are detected and reported promptly.	AS-3.1.1 Appropriate policies and procedures are established for application configuration management.	Inspect documented policies and procedures related to application change control procedures. Through inquiry and inspection, identify key transactions that provide user access to change application functionality. Inspect transaction reports of changes made to the application. For a sample of changes, inspect documentation of the changes made, including the validity, reasons, authorization, and the user authority. Note the handling of exceptions.

Exposure Draft

Control activities	Control techniques	Audit procedures
AS-3.2 Current configuration information is maintained.	AS-3.2.1 The entity maintains information on the current configuration of the application.	Review the entity's configuration management information.
AS-3.3 A system development life cycle methodology has been implemented.	AS-3.3.1 A SDLC methodology has been developed that <ul style="list-style-type: none">• provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process,• is sufficiently documented to provide guidance to staff with varying levels of skill and experience,• provides a means of controlling changes in requirements that occur over the system life, and• includes documentation requirements.	Review SDLC methodology. Review system documentation to verify that SDLC methodology was followed.
AS-3.4 Authorizations for changes are documented and maintained.	AS-3.4.1 change request forms are used to document requests and related projects. AS-3.4.2 Change requests must be approved by both system users and IT staff.	Identify recent software modification and determine whether change request forms were used. Examine a selection of software change request forms for approval.

Exposure Draft

Control activities	Control techniques	Audit procedures
AS-3.5 Changes are controlled as programs progress through testing to final approval.	<p>AS-3.5.1 Test plan standards have been developed for all levels of testing that define responsibilities for each party (e.g., users, system analysis, programmers, auditors, quality assurance, library control).</p> <p>AS -3.5.2 Detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.</p> <p>AS-3.5.3 Software changes are documented so that they can be traced from authorization to the final approved code.</p> <p>AS-3.5.4 Test plans are documented and approved that define responsibilities for each party involved.</p> <p>AS-3.5.5 Unit, integration, and system testing are performed and approved</p> <ul style="list-style-type: none">• in accordance with the test plan and• applying a sufficient range of valid and invalid conditions. <p>AS-3.5.6 A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing.</p> <p>AS-3.5.7 Test results are reviewed and documented.</p> <p>AS-3.5.8 Program changes are moved into production only upon documented approval from users and system development management.</p> <p>AS-3.5.9 Documentation is updated when a new or modified system is implemented.</p>	<p>Review test plan standards.</p> <p>Examine a selection of recent software changes and</p> <ul style="list-style-type: none">• review specifications;• trace changes from code to design specifications;• review test plans;• compare test documentation with related test plans;• analyze test failures to determine if they indicate ineffective software testing;• review test transactions and data;• review test results;• verify user acceptance; and• review updated documentation. <p>Determine whether operational systems experience a high number of abends and if so, whether they indicate inadequate testing prior to implementation.</p>

Exposure Draft

Control activities	Control techniques	Audit procedures
AS-3.6 Access to program libraries is restricted.	AS-3.6.1 Separate libraries are maintained for program development and maintenance, testing, and production programs.	Examine libraries in use.
	AS-3.6.2 Source code is maintained in a separate library.	Verify source code exists for a selection of production code modules by (1) comparing compile dates, (2) recompiling the source modules, and (3) comparing the resulting module size to production load module size.
	AS-3.6.3 Access to all programs, including production code, source code, and extra program copies are protected by access control software and operating system features.	For critical software production programs, determine whether access control software rules are clearly defined. Test access to program libraries by examining security system parameters.
AS-3.7 Movement of programs and data among libraries is controlled.	AS-3.7.1 A group independent of the user and programmers control movement of programs and data among libraries.	Review pertinent policies and procedures.
	Before and after images of program code are maintained and compared to ensure that only approved changes are made.	For a selection of program changes, examine related documentation to verify that <ul style="list-style-type: none"> procedures for authorizing movement among libraries were followed, and before and after images were compared.
AS-3.8 Access to application activities/ transactions is controlled via user roles (access privileges).	AS-3.8.1 User accounts are assigned to a role in the application. Roles are designed and approved by management to provide appropriate access and prevent an unauthorized user from executing critical transactions in production that change application functionality.	Inspect system reports and identify users who have access to configuration transactions. For a sample of users identified above, inspect user authorization forms to determine whether the user's access was authorized.
AS-3.9 Access to all application programs/codes and tables are controlled.	AS-3.9.1 Changes to application programs, codes and tables are either restricted or denied in the production environment. All changes are made using the approved change control process. User access to the application programs, codes, and tables is provided only for emergency user IDs.	Through inquiry and inspection, identify key programs and tables for the application. Inspect system reports of users with access to the key programs, codes and tables. Select a sample of users that have access to the identified programs and tables. Inspect documentation supporting how the access was provided. Note exceptions.

Exposure Draft

Control activities	Control techniques	Audit procedures
AS-3.10 Access to administration (system) transactions that provide access to table maintenance and program execution is limited to key users.	AS-3.10.1 Security design includes consideration for sensitive administration (system) transactions and restricted user access to these transactions.	<p>Inspect policies and procedures regarding restricted access to system administration transactions.</p> <p>Through inquiry and inspection, identify the system administration transactions.</p> <p>Inspect system reports of user access to these transactions.</p> <p>Select a sample of users with administration access and inspect documentation to determine whether access was authorized.</p> <p>Select a sample of system administration transactions executed by the system users and inspect resulting changes to the system elements, such as the program code or table.</p> <p>Inspect critical or privileged IDs (e.g., fire call ID) to determine if activity is logged.</p>
AS-3.11 Access and changes to programs and data are monitored.	AS-3.11.1 Procedures are established to reasonably assure that key program and table changes are monitored by a responsible individual who does not have the change authority. The procedures provide the details of reports/logs to run, specific valuation criteria and frequency of the assessment.	<p>Inspect documented procedures related to monitoring change control.</p> <p>Select a sample of reports or logs that are reviewed, and inspect to note evidence of monitoring compliance.</p>
AS-3.12 Changes are assessed periodically.	AS-3.12.1 Periodic assessment of compliance with change management process, and changes to configurable objects and programs.	<p>Inspect evidence of documented assessments performed.</p> <p>Determine who performed the assessment and note the exception handling procedures.</p>
AS-3.13 Applications are updated on a timely manner to protect against known vulnerabilities.	AS-3.13.1 The entity follows an effective process to identify vulnerabilities in applications and update them.	<p>Determine whether vendor supplied updates have been implemented.</p> <p>Assess management's process for identifying vulnerabilities and updating applications.</p>
AS-3.14 Emergency application changes are properly documented, tested, and approved.	AS-3.14.1 The entity follows an effective process to properly document, test, and approve emergency changes.	Inspect evidence of proper documentation, testing, and approval of emergency changes.

Source: GAO.

Exposure Draft

Critical Element – AS-4: Segregate user access to conflicting transactions and activities and monitor segregation

Effective segregation of duties is designed to prevent the possibility that a single person could be responsible for diverse and critical functions in such a way that errors or misappropriations could occur and not be detected in a timely manner, in the normal course of business processes. Although segregation of duties alone will not adequately assure that only authorized activities occur, inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. As discussed in AS-1, the security plan should address the organization-wide policy on segregation of duties (segregation of duty) and management should organize the user departments to achieve adequate segregation of duties. As part of this process, most organizations adopt segregation of duties control matrices as a guideline of the job responsibilities that should not be combined. It is important for the auditor to assess the relationship among various job functions, responsibilities and authorities in assessing adequate segregation of duties. The auditor starts this assessment with the review of the control matrices defined by management. Several automated tools are available to dynamically manage segregation of duty conflicts within an application. Appropriate business rules are critical to the effective implementation of these tools.

Entity management should consider the organization structure and roles in determining the appropriate controls for the relevant environment. For example, an organization may not have all the positions described in the segregation of duties matrix, or one person may be responsible for more than one of the roles described. Based on the organizational resource limitation and risk management, certain levels of segregation of duty conflicts may be allowed by management for a select role or users. If so, management should have appropriate compensating controls in place to mitigate the risks of allowing the conflicts.

Appropriate segregation of duties often presents difficulties in smaller organizations. Even entities or locations that have only a few employees, however, can usually divide their responsibilities to

Exposure Draft

achieve the necessary checks and balances. More often than not, the auditor will encounter situations where a few to substantial number of users may have access to activities with segregation of duty conflicts. Management generally mitigates the risks of allowing the segregation of duty conflicts by adding compensatory controls, such as approval of transactions before they are entered in the application or review of the posted transactions or reports as direct oversight and close monitoring of the incompatible activities. Typically, a combination of access and monitoring controls is necessary for design and operational effectiveness.

Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness when duties cannot be appropriately segregated. Compensating controls for segregation of duties conflicts generally include additional monitoring and supervision of the activities performed by the individual possessing conflicting responsibilities, and may include an additional level of required approval. The segregation of duty conflicts are mitigated to reduce or eliminate business risks through the identification of compensating controls.

Effective segregation of duties, consistent with Section 3.4, Segregation of Duties (SD), includes the following steps:

- Segregate user access to conflicting transactions and activities
- Monitor user access to conflicting transactions and activities through formal operating procedures, supervision, and review

Table 42. Control Techniques and Suggested Audit Procedures For Critical Element AS-4 - Segregate user access to conflicting transactions and activities and monitor segregation

Control activities	Control techniques	Audit procedures
AS-4.1 Incompatible activities and transactions are identified	AS-4.1.1 Owners have identified incompatible activities and transactions, and documented them on a segregation of duty matrix.	Through inquiry of management and inspection of policies and procedures, understand how management identifies incompatible activities and transactions.

Exposure Draft

Control activities	Control techniques	Audit procedures
	Owners have appropriately considered risk acceptance when allowing segregation of duty conflicts in user roles.	Inspect list of segregation of duty conflicts to determine whether management has identified the segregation of duty conflicts appropriate for the business process and considered risk acceptance when allowing the conflicts.
AS-4.2 Application controls prevent users from performing incompatible duties.	AS-4.2.1 Users are prevented by the application from executing incompatible transactions, as authorized by the business owners.	<p>Through inquiry, observation, and inspection, determine how the application segregates users from performing incompatible duties.</p> <p>Obtain and inspect a listing of users with access to the application. For a sample of users (can use same sample selected in AS-2.4.1, AS-2.4.3 & AS-2.6.3), inspect documentation to determine whether access to menus/ screens corresponds with the user's defined duties. Evaluate whether their duties and access is appropriate to prevent employees from performing incompatible duties.</p> <p>Specifically, perform the following steps:</p> <ul style="list-style-type: none"> ● Obtain a system-generated user listing for the application (and other applications, if applicable); ● For a selected sample of users, inspect their access profiles to determine whether access is appropriate (e.g., users have update access); and ● For the selected sample of users, inspect their access profiles to determine if any of the users have access to menus with conflicting duties.

Exposure Draft

Control activities	Control techniques	Audit procedures
AS-4.3.3 There is effective segregation of duties between the security administration function of the application and the user functions.	AS-4.3.1 The profiles for security administrators do not have privileges to input and/or approve transactions.	<p>Based on the inspection of user profiles, determine if:</p> <ul style="list-style-type: none"> • individuals with security administration functions have access to input, process, or approve transactions; • security administrators have access to more than application security administration functions; and • security administrators are prevented from accessing production data.
AS-4.4 User access to transactions or activities that have segregation of duties conflicts is appropriately controlled.	AS-4.4.1 Owners authorize users to have access to transactions or activities that cause segregation of duty conflicts only when supported by a business need.	<p>Inspect user administration policy to determine whether owner approval is required to access transactions or activities in their area of responsibility.</p> <p>Obtain and inspect a system report of users with conflicting responsibilities within the application. Obtain a sample of user access request forms (electronic documents/workflow, if applicable) and verify that the owners have approved user access to appropriate transactions or activities.</p>
	AS-4.4.2 Security Administrators review application user access authorizations for segregation of duties conflicts and discuss any questionable authorizations with owners.	Interview security administrators and observe and inspect relevant procedures and documentation. If the security administrator's review is documented on the request form, inspect a sample of forms to note evidence of the security administrator's review.
	AS-4.4.3 Owners periodically review access to identify unauthorized segregation of duties conflicts and determine whether any authorized segregation of duties conflicts remain appropriate.	Interview owners and inspect documentation; determine whether appropriate procedures are in place to identify and remove or modify access, as needed.
AS-4.5 Effective monitoring controls are in place to mitigate segregation of duty risks	AS-4.5.1 Process Owner has identified the segregation of duty conflicts that can exist, and the roles and users with conflicts.	Inspect documentation of roles and users with conflicts.

Exposure Draft

Control activities	Control techniques	Audit procedures
	AS-4.5.2 Documented monitoring controls are in place that specifically address the conflict that the control mitigates.	Identify segregation of duty conflicts (including those that were intentionally established by the entity) and review documentation to determine whether: <ul style="list-style-type: none"> • monitoring controls adequately mitigate the risks created by the segregation of duty conflict; and • monitoring controls are effective. This can be achieved by inspecting the evidence collected by management.
	AS-4.5.3 Management has documented evidence of monitoring of control effectiveness.	Review evidence of monitoring of control effectiveness.

Source: GAO.

Critical Element – AS-5: Implement effective application contingency planning

Chapter 3 addresses Contingency Planning at an entitywide and system level and is focused on the total information resources of an entity. Audit steps for the following section should be performed in conjunction with Chapter 3, which provides a more in-depth discussion of contingency planning issues. FISMA requires that each federal agency implement an information security program that includes “plans and procedures to ensure continuity of operations for information systems that support the operation and assets of the agency.” As shown in Chapter 3, an entity should

- Assess the criticality and sensitivity of computerized operations and identify supporting resources
- Take steps to prevent and minimize potential damage and interruption
- Develop and document a comprehensive contingency plan
- Periodically test the contingency plan and adjust it as appropriate

OMB Circular A-130, Appendix III, requires contingency plans for major applications, and NIST provides relevant guidance in Special

Exposure Draft

Publication 800-34, *Contingency Planning Guide for Information Technology Systems*.⁹²

Assess the criticality and sensitivity of the application

A key step in the contingency planning process is to conduct a Business Impact Analysis (BIA) for the application under focus.⁹³ The NIST contingency planning guide presents a three-step BIA process, which is discussed in Chapter 3 at the entitywide level. Following this process, staff conducting the BIA should, first, determine the critical functions performed by the application and then identify the specific IT resources required to perform the functions. Invariably, critical IT resources, in part, can include hardware and network components and telecommunication connections, as well as key application data and programs which should be backed up regularly. Second, staff should identify disruption impacts and allowable outage times for the application. And, third, staff should develop recovery priorities that will help determine recovery strategies. The NIST guide provides a range of recovery strategy considerations, including alternate sites of varying operational readiness, reciprocal agreements with other organizations, and service level agreements with equipment vendors.

Take steps to prevent and minimize potential damage and interruption.

The entity should implement policies and procedures to prevent or minimize potential damage and interruption to critical systems, including appropriate backup of application programs and data. Such policies and procedures should be incorporated into the entity's entitywide contingency planning efforts.

⁹² In addition, this Circular requires and the NIST guide recommends a plan for general support systems.

⁹³ NIST defines **Business Impact Analysis (BIA)** as follows: An analysis of an information technology (IT) system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Exposure Draft

Develop and document an application contingency plan.

A key step following the BIA, is to develop the application contingency plan (which NIST refers to as an IT contingency plan) and incorporate it into related plans. The NIST guide provides a discussion of various related types of plans, but recognizes that universally accepted definitions are not available, and the scope and purpose of a plan at an organization may vary from the definition provided in the NIST guide. The application contingency plan is focused on one application and may address recovery procedures at an alternative site. However, it probably will not address the recovery of a major processing facility supporting multiple applications, nor the continuity or recovery of business functions relying on multiple applications. Therefore, an entity's Disaster Recovery Plan for a major processing facility may cover multiple applications and establish recovery priorities by application. Likewise, an entity's business functions involving multiple applications may have Business Continuity and Recovery Plans that incorporate multiple contingency plans for applications. It is important that an application contingency plan be incorporated into broader-scoped, related plans so that the application receives proper priority among multiple applications. The application contingency plan should also include time-based implementation procedures so that recovery activities are performed in a logical sequence and reflect the application's allowable outage times to avoid significant impacts. Contingency plans should include consideration of alternate work sites.

No application contingency plan could be activated without the availability of key data and programs. Therefore, application data should be backed up regularly and current programs should be copied and available for use. Both should be safeguarded, stored offsite, and be retrievable when recovery actions are implemented. The NIST guide provides a discussion of backup methods and considerations.

The entity should prevent and minimize potential damage and interruption. Chapter 3 includes a discussion of steps as the entitywide and system levels. In addition, for applications, the entity should maintain appropriate backup of applications and application data. Also, it is important that restarts process data completely and

Exposure Draft

accurately. Further, when an application contingency plan has been activated, responsible contingency personnel should reasonably assure that effective controls will restrict and monitor user access to application data and programs during the contingency operation. If adequate preparations have not been made or proper procedures are not followed, the contingency plan activation could result in an operational application with vulnerabilities that might allow unauthorized access to data and programs. As examples, access control software may not be started or allow default passwords, outdated software lacking up to date patches and containing known weaknesses may be activated, and logging of auditable events may not occur.

The control environment for the contingency operation should be similar to the normal operation. In particular, access controls as specified in the previous section AS-2 should be operating. That is, contingency operations should provide for effective user identification and authentication, proper authorization to perform sensitive transactions, and a continuing audit and monitoring capability.

Periodically test the contingency plan and adjust it as appropriate.

Testing the application contingency plan is essential to ensure it will function as intended when activated for an emergency. Testing can reveal important weaknesses. Testing the contingency plan and making adjustments as needed helps ensure the application will work when the contingency plan is implemented for an actual emergency. The NIST contingency planning guide recommends the following areas to be addressed in a contingency test:

- System recovery on an alternate platform from backup media
- Coordination among recovery teams
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations
- Notification procedures

Exposure Draft

NIST's Handbook on Computer Security⁹⁴ discusses various degrees of contingency plan tests that could range from 1) a simple accuracy review to determine that key personnel contacts are still employed by the entity to 2) disaster simulations. On disaster simulations, this Handbook states the following: "These tests provide valuable information about flaws in the contingency plan and provide practice for a real emergency. While they can be expensive, these tests can also provide critical information that can be used to ensure the continuity of important functions. In general, the more critical the functions and the resources addressed in the contingency plan, the more cost-beneficial it is to perform a disaster simulation."

The NIST contingency planning guide states that test results and lessons learned should be documented and reviewed. The guide further states that, to be effective, the plan should be maintained in a ready state that accurately reflects the system, requirements, procedures, organizational structure, and policies and, therefore, the plan should be reviewed and updated regularly, at least annually or whenever significant changes occur.

⁹⁴ Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*

Exposure Draft

Table 43. Control Techniques And Suggested Audit Procedures For Critical Element AS-5 – Maintain an effective contingency planning program

Control activities	Control techniques	Audit procedures
AS-5.1 Assess the criticality and sensitivity of the application through a Business Impact Analysis (BIA) or equivalent.	AS-5.1.1 Determine the critical functions performed by the application and identify the IT resources, including key data and programs, required to perform them.	Review the policies and methodology, and the BIA (if conducted) used to determine the application's critical functions and supporting IT resources, the outage impacts and allowable outage times, and the recovery priorities.
	AS-5.1.2 Identify the disruption impacts and allowable outage times for the application.	
	AS-5.1.3 Develop recovery priorities that will help determine recovery strategies.	Interview program, information technology, and security administration officials. Determine their input and assessment of the reasonableness of the results.
AS-5.2 Take steps to prevent and minimize potential damage and interruption.	AS-5.2.1 Backup files of key application data are created on a prescribed basis.	Review written policies and procedures for backing up and storing application data and programs.
	AS-5.2.2 Current application programs are copied and available for use	Examine the backup storage site.
	AS-5.2.3 Backup files of application data and programs are securely stored offsite and retrievable for contingency plan implementation	Interview program and information technology officials and determine their assessment of the adequacy of backup policy and procedures.
AS-5.3 Develop and document an application Contingency Plan	AS-5.3.1 Develop a time-based application Contingency Plan.	Review the application contingency plan and broader scoped related plans.
	AS-5.3.2 Incorporate the application Contingency Plan into related plans, such as the Disaster Recovery, Business Continuity, and Business Resumption Plans.	Determine whether the broader-scoped plans have incorporated the application contingency plan. Compare the plan with guidance provided in NIST SP 800-34.
	AS-5.3.3 Contingency operations provide for an effective control environment by restricting and monitoring user access to application data and programs, including. <ul style="list-style-type: none"> • Users are identified and authenticated. • Users are properly authorized before being able to perform sensitive transactions. • Audit and monitoring capabilities are operating. 	Interview program, information technology, and security administration officials and determine their input and assessment of the reasonableness of the plan. Review the contingency plan and any test results for control related issues.

Exposure Draft

Control activities	Control techniques	Audit procedures
AS-5.4 Periodically test the application contingency plan and adjust it as appropriate.	AS-5.5.1 The application contingency plan is periodically tested and test conditions include disaster simulations.	Review policies on testing. Determine when and how often contingency plans are tested.
	AS-5.5.2 The following areas are included in the contingency test: <ul style="list-style-type: none"> • System recovery on an alternate platform from backup media • Coordination among recovery teams • Internal and external connectivity • System performance using alternate equipment • Restoration of normal operations • Notification procedures 	Determine if technology is appropriately considered in periodic tests of the contingency plan and resultant adjustments to the plan. Review test results. Observe a disaster recovery test.
	AS-5.5.3 Test results are documented and a report, such as a lessons-learned report, is developed and provided to senior management.	Review the final test report. Interview senior management to determine whether they are aware of the test results.
	AS-5.5.4 The contingency plan and related agreements and preparations are adjusted to correct any deficiencies identified during testing.	Review any documentation supporting contingency plan adjustments.

Source: GAO.

Exposure Draft

4.2. Business Process Controls (BP)

Business Process controls are the automated and/or manual controls applied to business transaction flows and relate to the completeness, accuracy, validity and confidentiality of transactions and data during application processing. They typically cover the structure, policies, and procedures that operate at a detailed business process (cycle or transaction) level and operate over individual transactions or activities across business processes. Specific types of business process controls are:

- **Transaction Data Input** relates to controls over data that enter the application (e.g., data validation and edit checks).
- **Transaction Data Processing** relates to controls over data integrity within the application (e.g., review of transaction processing logs).
- **Transaction Data Output** relates to controls over data output and distribution (e.g., output reconciliation and review).
- **Master Data Setup and Maintenance** relates to controls over master data, the key information that is relatively constant and shared between multiple functions or applications (e.g., vendor file).

The particular control techniques employed by an entity will depend on the context of the business process and its associated risks and objectives. Business process controls may be manual or automated. Automated controls are system-based, and may be used to control such things as the correctness or accuracy of data, such as edits and validations. Manual controls are procedures that require human intervention, such as the approval of a transaction, and are typically used to assure the reasonableness or propriety of transactions. Automated and manual controls can be preventive or detective. Automated controls can keep invalid data from being processed, and they can report transactions that fail to meet reasonableness criteria. Manual controls performed prior to input can identify problems before data is processed, while monitoring controls performed after processing can identify errors.

Exposure Draft

In many entities, the core business processes span across multiple applications. Some of the applications are themselves complex, integrated systems. Ideally, applications are interfaced seamlessly for the information to flow across these applications to complete a business process. Furthermore, functional areas may expand outside of the organization to include external “partners” as part of a larger vendor/contract management or personnel management, wherein partner applications are often interfaced with entity systems. This expansion of the environment to include external systems adds to the risks or challenges faced by the organization. If not properly controlled, these interfaces with external “partners” can affect the confidentiality, integrity, and availability of information and information systems.

At a high level, execution of a business process involves data input, processing and data output. However, the characteristics of data types (master or standing data and transaction data), and the complexity of the interfaced systems and the underlying data management systems, require the auditor to consider these in evaluating the completeness, accuracy, validity and confidentiality of data.

Master Data vs. Transaction Data

Every business process employs **master data**, or referential data that provides the basis for ongoing business activities, e.g., customers, vendors, and employees. The data that are generated as a result of these activities are called **transaction data**, and represent the result of the activity in the form of documents or postings, such as purchase orders and obligations.

Examples of master data are:

- Organizational structure
- G/L Account Structure
- Vendor Master
- Employee Master

Exposure Draft

Financially focused master data generally has the following characteristics:

- Relatively stable over time; even if the data records change, the overall volume of growth is limited. Example: chart of accounts, fixed assets, and vendors.
- Occur only once per object in the application. Example: assets are used by almost every organizational unit, but there is only one master record per asset.
- Everything else depends on them, e.g. inventory balances cannot be loaded without the organizational structure, G/L accounts, and material master being loaded. Therefore, master data should be loaded prior to processing business transactions.

Business Process Control Objectives

As discussed in the introduction to this chapter, the overall objectives of business process application level controls are to reasonably assure completeness, accuracy, validity and confidentiality of transactions and data during application processing. In particular, each specific business process control technique is designed to achieve one or more of these objectives. The effectiveness of business process controls depends on whether all of these overall objectives are achieved by the application level controls. Each objective is described in more detail below.

Completeness (C) controls should provide reasonable assurance that all transactions that occurred are input into the system, accepted for processing, processed once and only once by the system, and properly included in output. Completeness controls include the following key elements:

- transactions are completely input,
- valid transactions are accepted by the system,
- duplicate postings are rejected by the system,

Exposure Draft

- rejected transactions are identified, corrected and re-processed; and
- all transactions accepted by the system are processed completely.

The most common completeness controls in applications are batch totals, sequence checking, matching, duplicate checking, reconciliations, control totals and exception reporting.

Accuracy (A) controls should provide reasonable assurance that transactions are properly recorded, with the correct amount/data, and on a timely basis (in the proper period); key data elements input for transactions are accurate; and data elements are processed accurately by applications that produce reliable results; and output is accurate.

Accuracy control techniques include programmed edit checks (e.g., validations, reasonableness checks, dependency checks, existence checks, format checks, mathematical accuracy, range checks, etc.), batch totals and check digit verification.

Validity (V) controls should provide reasonable assurance (1) that all recorded transactions actually occurred (are real), relate to the organization, and were properly approved in accordance with management's authorization; and (2) that output contains only valid data. A transaction is valid when it has been authorized (for example, buying from a particular supplier) and when the master data relating to that transaction is reliable (for example, the name, bank account and other details on that supplier). Validity includes the concept of authenticity. Examples of validity controls are one-for-one checking and matching.

Confidentiality (CF) controls should provide reasonable assurance that application data and reports and other output are protected against unauthorized access. Examples of confidentiality controls include restricted physical and logical access to sensitive business process applications, data files, transactions, and output, and adequate segregation of duties. Confidentiality also includes

Exposure Draft

restricted access to data reporting/extraction tools as well as copies or extractions of data files.

NIST Guidance

For federal systems, NIST SP 800-53 includes the following controls related to business process controls:

SI-9 Information Input Restrictions SI-10 Information Accuracy, Completeness, Validity, and Authenticity SI-11 Error Handling SI-12 Information Output Handling and Retention
--

This section presents more detailed control objectives that should be achieved to reasonably assure that transaction data is complete, accurate, valid and confidential. Also, this section is organized to address the four principal types of business process controls: input, processing, output, and master files.

Business Process Control Critical Elements

Business Process Controls have the following four critical elements:

BP-1	Transaction Data Input is complete, accurate, valid, and confidential (Transaction data input controls).
BP-2	Transaction Data Processing is complete, accurate, valid, and confidential (Transaction data processing controls).
BP-3	Transaction Data Output is complete, accurate, valid, and confidential (Transaction data output controls).
BP-4	Master data setup and maintenance is adequately controlled.

BP-1 Transaction Data Input is complete, accurate, valid, and confidential (Transaction Data Input Controls)

The entity should implement procedures to reasonably assure that (1) all data input is done in a controlled manner, (2) data input into the application is complete, accurate, and valid, (3) any incorrect information is identified, rejected, and corrected for subsequent

Exposure Draft

processing, and (4) the confidentiality of data is adequately protected. Inadequate input controls can result in incomplete, inaccurate, and/or invalid records in the application data or unauthorized disclosure of application data.

Applications can accept input manually (application users enter data), or via automated input. The automated input may be interfaces that use batch processing or are integrated real-time with internal and external systems. To the extent that data input is obtained from other applications, the auditor's assessment of input controls should be coordinated with data interface controls discussed in section 4.3 of this chapter.

For federal systems, NIST SP 800-53 [SI-10] establishes the following objectives for input controls:

- checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible.
- rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content.
- inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.

Also, SI-10 states that the extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.

Data input for processing should have all key fields completed and be validated and edited. Error handling procedures should facilitate timely resubmission of corrected data, including real-time on-line edits and validations. These controls may be configured within the system settings, or added on as a customization. Where applicable, the auditor may also process a controlled group of live data and test for expected results. Preventive controls generally allow for higher reliance and the most efficient testing.

Exposure Draft

In addition, controls should be in place to reasonably assure that access to data input is adequately controlled. Procedures should be implemented to control access to application input routines and physical input media (blank and completed). The assessment of such controls should be coordinated with Critical Element AS-2 *Implement effective application access controls.*

For federal systems, NIST SP 800-53 includes three controls relevant to transaction data input:

SI-9 Information Input Restrictions SI-10 Information Accuracy, Completeness, Validity, and Authenticity SI-11 Error Handling

Data input controls are comprised of the following control activities:

- Implement an effective transaction data strategy and design
- Establish input preparation (approval and review) policies and procedures
- Build data validations and edit checks into the application
- Implement effective auditing and monitoring capability

Implement an effective transaction data strategy and design

The entity should have an appropriate data strategy and design (how the data are organized into structures to facilitate retrieval while minimizing redundancy). The design of transaction data elements is a critical factor in helping to assure the quality of data as well as its interrelationship with other data elements. Data standards⁹⁵ should be defined and maintained, but may vary depending upon the

⁹⁵ Data standards are designed to enable systems to easily interoperate and transfer information. Standard definitions for data elements are intended to ensure that users of all entity systems define the same data in the same way and have a common understanding of their meaning.

Exposure Draft

specific requirements of the entity, including regulatory requirements, and database- or application-based standards.

A clearly defined data strategy minimizes data redundancies fundamental to an efficient, effective transaction processing function. Poor data quality may lead to a failure of system controls, process inefficiencies, and inaccurate management reporting. Erroneous or missing elements of critical data in the transaction file can produce discrepancies within the process cycle.

Characteristics of erroneous transaction file data elements include, but are not limited to, duplicate transactions recorded or processed, and improper coding to departments, business units or accounts. They also include unpopulated data fields and data formatting inconsistencies, as described for the master file.

Establish Input Preparation (approval and review) Policies and Procedures

The entity should have policies and procedures in place to reasonably assure that all authorized source documents and input files are complete and accurate, properly accounted for, and transmitted in a timely manner for input to the computer system. Among these, management should establish procedures to reasonably assure that all inputs into the application have been processed and accounted for; and any missing or unaccounted for source documents or input transactions have been identified and investigated. Finally, procedures should be established to reasonably assure that all source documents (paper or electronic form) have been entered and accepted to create a valid transaction. Automatic input from other applications should be integrated either through an interface (external applications) or configuration (cross-modular within the same application). Interface controls are addressed in section 4.3, below.

For federal systems, NIST SP 800-53 [SI-9] establishes a control objective that the organization restricts the capability to input information to the information system to authorized personnel. Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Exposure Draft

Build Data Validation and Edits within the Application

Input data should be validated and edited to provide reasonable assurance that erroneous data are prevented or detected before processing. In many cases, application owners and programmers will build application input edits directly into the application to limit the number of errors that are input into the application. Edits are used to help assure that data are complete, accurate, valid, and recorded in the proper format. Edits can include programming to identify and correct invalid field lengths or characters, missing data, incorrect data, or erroneous dates. The auditor should obtain an understanding of the application input edits to assess their adequacy and to determine the edits that will be tested.

Implement Effective Auditing and Monitoring Capability

As part of the data input process, data entry errors may occur. These errors can occur during manual or automated entry of data. Management should have procedures to identify and correct any errors that occur during the data entry process. Error handling procedures during data entry should reasonably assure that errors and irregularities are detected, reported, and corrected. Management's audit and monitoring capability should include

- user error logs to provide timely follow-up and correction of unresolved data errors and irregularities, and
- an established monitoring process to assure the effectiveness of error handling procedures.

For federal systems, NIST SP 800-53 [SI-11] states that the information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and

Exposure Draft

handle error conditions is guided by organizational policy and operational requirements.

Table 44. Control Techniques And Suggested Audit Procedures For Critical Element BP-1 - Transaction Data Input is complete, accurate, valid, and confidential.

Control activity	Control Object.	Control techniques	Audit procedures
BP-1.1 A transaction data strategy is properly defined, documented, and appropriate.	C,A,V, CF	BP-1.1.1 Data management procedures exist that include transaction data strategy, data design, data definitions, data quality standards, ownership and monitoring procedures. Data strategy should be unique to each data type.	Inquire of management and inspect documented policies and procedures related to data strategy. Inspect transaction data strategy.
BP-1.2 Source documentation and input file data collection and input preparation and entry is effectively controlled.	C,V,CF	BP-1.2.1 Procedures are established to provide reasonable assurance that all inputs into the application have been authorized, accepted for processing, and accounted for; and any missing or unaccounted for source documents or input files have been identified and investigated. Such procedures may include one or more of the following: <ul style="list-style-type: none"> • batch totals • sequence checking • reconciliations • control totals 	<p>Through inquiry, observation, and inspection, obtain an understanding of policies and procedures related to source document and input file collection and preparation, and determine whether the procedures are documented and properly designed.</p> <p>Observe and inspect input preparation policies and procedures and relevant controls, noting procedures taken when exceptions are identified.</p> <p>Inspect a selection of reports (a sample is not required, but the auditor could elect to choose one) used by management to determine whether the necessary inputs are accepted for processing, and inquire of review procedures used.</p> <p>Inquire as to how source documents and input files are tracked and maintained and inspect relevant documentation.</p>
BP-1.3 Access to data input is adequately controlled	C,A,V, CF	BP-1.3.1 Procedures are implemented to control access to application input routines and physical input media (blank and completed)	Review procedures over control of data input to determine whether they are adequate. Coordinate this step with AS-2.

Exposure Draft

Control activity	Control Object.	Control techniques	Audit procedures
BP-1.4 Input data are approved	A, V	BP-1.4.1 Documented approval procedures exist to validate input data before entering the system. Approval procedures are followed for data input.	Inspect documented procedures for approval of input data. Inspect a selection of source documents (a sample is not required, but auditor could elect to choose one) and input files and determine whether the source data were approved for input.

Exposure Draft

Control activity	Control Object.	Control techniques	Audit procedures
BP-1.5 Input data are validated and edited to provide reasonable assurance that erroneous data are detected before processing.	A,V	<p>BP-1.5.1 Appropriate edits are used to reasonably assure that data are valid and recorded in the proper format, including:</p> <ul style="list-style-type: none"> • authorization or approval codes; • field format controls; • required field controls; • limit and reasonableness controls; • valid combination of related data field values; • range checks • mathematical accuracy • master file matching • duplicate processing controls; and • balancing controls. 	<p>Through inquiry, observation, and inspection, understand edits used to reasonably assure that input data is accurate, valid, and in the proper format prior to being accepted by the application. The edits and procedures should address both manual and automated input processes.</p> <p>Identify the key data input screens. Consider such factors as known errors and the frequency of use. If available, use analytical reports to support reasoning for screen selection. For the key manual input layouts identified, perform the following steps as applicable:</p> <ul style="list-style-type: none"> • Observe an authorized data entry clerk inputting transactions, noting edits and validations for the various transaction entries. • Observe key transaction fields to determine whether they have adequate edit/validation controls over data input. • Obtain screen prints of appropriate scenarios and document the result. <p>For key automated inputs, observe and inspect data validation processes, completion controls, and exception reports in place. Inquire of management regarding procedures used to reject and resubmit data for processing, and procedures to provide reasonable assurance that data is not processed multiple times.</p> <p>Note: audit procedures apply only to the current environment at the time of test. Supplemental audit procedures would need to be applied at other points during the year to obtain evidence that the control was operating effectively.)</p>

Exposure Draft

Control activity	Control Object.	Control techniques	Audit procedures
		<p>BP-1.5.2 Edit and validation overrides are restricted to authorized personnel.</p> <p>Procedures exist to monitor, in a timely manner, overrides applied to transactions.</p>	<p>Observe and inspect existing procedures for reviewer overrides or bypassing data validation and error routines. If an override log exists, observe and inspect to determining whether adequate review and follow up of overrides is performed.</p> <p>Inspect a selection of overrides for evidence of proper approval. (Note: use of overrides is not by itself indicative of inadequate controls. However, the auditor needs to examine why the overrides are being used and controls in place to minimize risks from these actions).</p>
		<p>BP-1.5.3 Table maintenance procedures include edit and validation controls to help assure that only valid changes are made to data tables.</p>	<p>Through inquiry, observation, and inspection, obtain an understanding of table maintenance procedures relative to data edits and validation.</p> <p>Observe an authorized person attempting to make invalid changes to tables, and confirm edits and validations are performed on changes.</p>
<p>BP-1.6 Input values to data fields that do not fall within the tolerances or parameters determined by the management result in an input warning or error.</p>	A,V	<p>BP-1.6.1 Parameters and tolerances are configured and error conditions and messages are defined. (These restrictions can be configured based on limits on transaction amounts or based on the nature of transactions)</p>	<p>Inspect configuration of parameters and tolerance levels defined by the entity to identify whether the application accepts the data with warning or rejects the data, if the conditions are not met.</p>
		<p>If a workflow is used so that documents can be released only by personnel with appropriate approval authority, then these requirements should be appropriately designed in the system.</p>	<p>Inspect management review procedures, if the application accepts user data, with a warning.</p> <p>Inspect the workflow rules and validate that the releasing authority is at an appropriate level.</p>
		<p>Management regularly reviews the restrictions placed on data input and validates that they are accurate and appropriate.</p>	<p>Inspect evidence of management's regular review of relevant tolerances and parameters, and any correctional activities taken.</p>

Exposure Draft

Control activity	Control Object.	Control techniques	Audit procedures
BP-1.7 Error handling procedures during data origination and entry reasonably assure that errors and irregularities are detected, reported, and corrected.	C,A,V	BP-1.7.1 Procedures are established to reasonably assure that all inputs into the application have been accepted for processing and accounted for; and any missing or unaccounted for source documents or input files have been identified and investigated. The procedures specifically require the exceptions to be resolved within a specific time period.	<p>Inspect documented procedures related to data entry error handling procedures.</p> <p>Inquire of management to determine which key management reports are used to monitor input errors.</p> <p>Select a sample of input error reports and inspect to note evidence of management review. As applicable, inspect subsequent data input reports to note where data was corrected and resubmitted for processing.</p>
BP-1.8 Errors are investigated and resubmitted for processing promptly and accurately.	C,A,V	BP-1.8.1 Data input errors are identified in suspense or error reports and resolved or resubmitted in a timely manner (within the period specified in the procedures).	<p>Inspect a sample of recent suspense or error reports (can use sample selected in BP-1.7.1 provided information included will satisfy audit objectives for both audit procedures) and note whether suspense items are being corrected in a timely manner. Inspect the open items and note management's reasons for not correcting them in a timely manner.</p>

Source: GAO.

BP-2 Transaction Data Processing is complete, accurate, valid, and confidential (Transaction Data Processing Controls)

Transaction data processing controls address the completeness, accuracy, validity, and confidentiality of data as the data get processed within the application. Data processing controls are employed following input, or during batch processing or on-line user processing within the application.

Once the initial data are entered in the system and accepted for processing, the processing of the data should be controlled by a series of activities within the system. These activities are designed by management and are either programmed or configured into the application. The processing steps are different for each process (purchasing versus invoice processing) and control requirements differ to mitigate the risks inherent to the applicable process. An effective assessment of data processing controls includes an understanding of the process steps and dataflow in a process cycle,

Exposure Draft

the controls imbedded in the application, and the manual controls that are common across processes or specific to each process.

Some applications may allow user-defined processing, whereby the user may establish or modify processing. This frequently occurs in applications based on spreadsheets and report writer/data extraction tools. Entities should establish clear policies and procedures concerning user-defined processing. In addition, the entity should have adequate controls over the accuracy, completeness and validity of information processed in applications with user-defined processing.

Audit trails and security reports should be monitored on a regular basis to help assure that transactions are processing as intended. The effectiveness of such procedures depends on the level of security reporting and problem analysis tools available in the application. Controls over the processing of data should preclude or detect the erroneous or unauthorized addition, removal, or alteration of data during processing.

Interface controls relate to the integrity of data as they move from one system to another. Interface controls are addressed separately in Section 4.3 below.

For federal systems, as noted in BP-1 above, NIST SP 800-53 includes three controls relevant to data processing:

SI-9 Information Input Restrictions SI-10 Information Accuracy, Completeness, Validity, and Authenticity SI-11 Error Handling

Formal Transaction Processing Procedures.

Formal procedures should be established for data processing to help assure that data are processed completely and accurately, that data retains its validity, and that appropriate data confidentiality is maintained during processing. Related controls include the following:

Exposure Draft

- Transaction or table logs provide an audit trail and the ability to compare transactions to source documents. Audit trails or processing logs are often used within applications to track the pertinent information related to application transactions, both manual and automated. The processing logs should also be used to identify those transactions that did not process completely or correctly within the application. The log should document the errors identified during application processing, and should contain enough information for the systems personnel to identify the exact transactions that failed, and the application users that will need to be contacted to correct the posting (if the error can not be corrected by the systems personnel). Processing logs typically contain such information as date and time of error, responsible user (if applicable), codes describing the type of error encountered, and the corrective action that has occurred to assure correct processing of the transaction.
- An automated process exists that allows one or more of the following: capturing transaction data in correct accounts; unique documentation; tolerances in processing data; periodic review and reconciliation of subsidiary or clearing accounts (e.g., clearing Goods Received accounts against Invoice Received accounts through two- and three-way matching process); prevention of direct posting to reconciliation accounts; and workflow to initiate the approval process.
- Efficient transaction entry that eliminates unnecessary duplication of data entry. Where appropriate, data needed by the systems are entered only once and other parts of the system are automatically updated consistent with the timing requirements of each process cycle.
- Managers should provide review and authorization for transactions that are rejected and should be rerun.

Effective auditing and monitoring capability.

During data processing, transactions may not be processed completely or accurately as a result of errors or inconsistencies in data, system interruptions, communication failures, or other events. In addition, valid data may be corrupted or data may lose its

Exposure Draft

confidentiality. To identify these instances, a monitoring capability should be implemented. The monitoring function should reasonably assure that data are accurately processed through the application and that processing procedures determine data to be added, or altered during processing. No data should be lost during the process. Controls may include:

- If the application is “run” on a regular schedule to process data, either manually or automatically, there are documented procedures explaining how this is performed, including controls in place to reasonably assure that all processing was completed.
- A processing log is maintained and is reviewed on a regular basis for unusual or unauthorized activity.
- The processing log, or another log or report, is used to document any errors or problems encountered during processing. Types of information that should be considered for retention are descriptions of any errors encountered, dates identified, any codes associated with errors, any corrective action taken, date and times corrected.
- controls to reasonably assure that the correct generation/cycle of files is used for processing. This may include the generation of backup files from processing to be used for disaster recovery.
- Adequate audit trails are generated during processing. These audit trails should be logs or reports that contain information about each transaction. Data that should be included are who initiated each of the transactions, the date and time of the transactions, and the location of the transaction origination (terminal or IP address as an example).

Exposure Draft

Table 45. Control Techniques And Suggested Audit Procedures For Critical Element BP-2 Transaction Data Processing is complete, accurate, valid, and confidential.

Control activity	Control Object.	Control techniques	Audit procedures
BP2.1 Application functionality is designed to process input data, with minimal manual intervention.	C,A,V, CF	<p>BP-2.1.1 Application processing of input data is automated and standardized.</p> <p>Design documentation supporting the processing design exists for validation and change control purposes.</p> <p>The version of application, data and files to be processed are appropriate and current.</p>	<p>Inspect configuration and/or design documentation noting automatic and manual processing of transaction and information flow. Verify that proper versions of application, data and file are used.</p>
BP-2.2 Processing errors are identified, logged and resolved.	C, A, V	<p>BP-2.2.1 System entries use transaction logs to reasonably assure that all transactions are properly processed and identify the transactions that were not completely processed.</p> <p>BP-2.2.2 Procedures are in place to identify and review the incomplete execution of transactions, analyze and take appropriate action.</p> <p>BP-2.2.3 Procedures exist to monitor, in a timely manner, overrides applied to transaction processing.</p>	<p>Inspect a selection of application, transaction and error logs, noting whether all transactions were properly processed and missing or duplicate transactions were identified, including reruns and restarts.</p> <p>Inspect selected incomplete transactions and validate that management has adequately investigated and corrected the errors or omissions.</p> <p>Conduct a test with controlled group of live data and analyze the results with the expected values. Follow up with any exceptions.</p> <p>Observe and inspect existing procedures for reviewer overrides or bypassing data processing routines. If an override log exists, observe and inspect to determining whether adequate review and follow up of overrides is performed.</p> <p>Inspect a selection of overrides for evidence of proper approval. (Note: use of overrides is not by itself indicative of inadequate controls. However, the auditor needs to examine why the overrides are being used and controls in place to minimize risks from these actions).</p>

Exposure Draft

Control activity	Control Object.	Control techniques	Audit procedures
BP-2.3 Transactions are executed in accordance with the pre-determined parameters and tolerances, specific to entity's risk management.	A,V	BP-2.3.1 Document processing and posting conditions (parameters and tolerances) are configured, including system errors and actions, if the are conditions are not met.	Inspect configuration of parameters and tolerances levels defined by the entity to identify whether the application processes the data with warning or rejects the data, if the conditions are not met.
		BP-2.3.2 Management regularly reviews the restrictions to validate the accuracy and appropriateness.	Inspect management review procedures, noting management action when the application processes data or rejects it. In both cases, management should clearly analyze the impact on the downstream transactions.
BP-2.4 Transactions are valid and are unique (not duplicated).	A, V	BP-2.4.1 The application performs on-line edit and validation checks against data being processed.	Inspect design document to identify key data validation and edit checks.
		BP-2.4.2 The system produces warning or error messages.	Inspect configuration to verify that the identified edit and validations checks are appropriately set, and transactions are rejected/suspended when data/processing errors occur. Also verify that warning and error messages are designed when the processing is incomplete.
		BP-2.4.3 Transactions with errors are rejected or suspended from processing until the error is corrected.	
		BP-2.4.4 The application communicates the processing error to the Users either on-line (if on-line entry) or via an exception report.	Inspect the error communication methodology.
BP-2.5 The transactions appropriately authorized.	A,V	BP-2.5.1 Transactions are matched with management's general or specific authorizations.	Review the adequacy of controls over authorization of transactions.
BP-2.6 Data from subsidiary ledgers are in balance with the general ledger (step applicable to financial-related audits only).	C,A,V	BP-2.6.1 Periodic reconciliation is performed and exceptions are appropriately handled.	Inspect periodic procedures to determine whether reconciliations are performed and documented with evidence.
			For a selection of reconciliations, examine supporting evidence for adequacy.
			Through inquiry, observations, and inspection, determine if the system is configured to auto balance, where possible.

Exposure Draft

Control activity	Control Object.	Control techniques	Audit procedures
BP-2.7 User-defined processing is adequately controlled.	C, A, V, CF	BP-2.7.1 Appropriate policies and procedures over user-defined processing are implemented.	Review policies and procedures over user-defined processing.
		BP-2.7.2 Controls over user-defined processing are adequate.	Assess the operating effectiveness of user-defined processing.
BP-2.8 As appropriate, the confidentiality of transaction data during processing is adequately controlled	CF	BP-2.8.1 Management implements adequate controls to protect the confidentiality of data during processing, as appropriate.	Assess the adequacy of management controls over confidentiality during processing.
			Coordinate this step with Critical Element AS-2 <i>Implement effective application access controls.</i>
BP-2.9 An adequate audit and monitoring capability is implemented.	C,A	BP-2.9.1 Management has procedures in place to reconcile the data input with the data processed by the application.	Inspect procedures regarding reconciliation of transactions.
		BP-2.9.2 Monitoring procedures should provide details of data to be added/modified during the processing, and expected result. System audit logs should be reviewed for exception.	Inspect operations activity at selected times and check for evidence that reconciliations are being performed.
		BP-2.9.3 Management maintains a process log and the log is reviewed for unusual or unauthorized activity.	Inspect the processing log and note whether the unusual or unauthorized activity was followed up properly and promptly.

Source: GAO.

BP-3 Transaction data output is complete, accurate, valid, and confidential (Transaction Data Output Controls)

Like input and processing controls, transaction data output controls are used to reasonably assure that transaction data is complete, accurate, valid, and confidential. In addition, output controls are aimed at the correct and timely distribution of any output produced. Output can be in hardcopy form, in the form of files used as input to other systems, or information available for online viewing.

Formal procedures should be established for data processing to help assure that data are processed completely and accurately, that data retains its validity, and that appropriate data confidentiality is maintained during processing.

Exposure Draft

Formal procedures should be established for data processing to help assure that data are processed completely and accurately, that data retains its validity, and that appropriate data confidentiality is maintained during processing, output control totals are accurate and are being verified, and the resulting information is distributed in a timely and consistent manner to the appropriate end users. Controls include:

- An overall reporting process that identifies specific output that will be generated, the form and content of the reporting, sensitivity of information and selectivity of user.
 - Output is delivered to the appropriate end user.
 - Output is restricted from unauthorized access.
 - Record retention and backup schedules for output data should be established.
- Data integrity through reconciliation of the output to the input and processing data.
 - Documented procedures explain the methods for the proper balancing/reconciliation and error correcting of output should exist. There should be adequate separation of duties for the balancing/reconciliation process.
 - Output is reviewed for general acceptability and completeness, including any control totals. There should be either error reports or a log kept of output errors. These should contain information such as a description of problems/errors and the date identified, as well as any corrective action taken.

In addition, controls should be in place to reasonably assure that access to data output is adequately controlled. Procedures should be implemented to control access to output data and physical output media (blank and completed). The assessment of such controls should be coordinated with Critical Element AS-2 *Implement effective application access controls.*

Exposure Draft

For federal systems, as noted in BP-1 above, NIST SP 800-53 includes three controls relevant to data output controls:

SI-9 Information Input Restrictions
SI-10 Information Accuracy, Completeness, Validity, and Authenticity
SI-11 Error Handling

In addition, NIST SP 800-53 [SI-12] states that the organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Implementing a reporting strategy

One of the key elements of output controls is having an overall reporting strategy. The strategy helps to reasonably assure that content and availability of reports is consistent with end users' needs, that end users are aware of the sensitivity and confidentiality of data, and that an "owner" has been defined for all report output. The strategy also provides a basis for policies and procedures that govern preferred report methods (hardcopy vs. soft, standard vs. custom), report generation and distribution, and any review and or approvals.

The strategy should specifically consider:

- Compliance with laws and regulations;
- Sensitivity of data;
- Levels of reporting segregation of duties;
- Consolidation/ processing of reporting from a 3rd party;
- Reporting tools utilized;
- Business needs/functionality of reports; and
- Non-standard output items.

Exposure Draft

The strategy should adequately consider the confidentiality of all types of output. For example, the entity should have adequate security over output queues, particularly for sensitive information. Inadequately secured output queues can lead to unauthorized disclosure of information. Similarly, access to output screens should be adequately controlled.

Another significant area for output controls relates to data that is routinely or episodically transferred to other systems, such as data supporting a management reporting system. If controls over such other systems are not adequate and consistent with the risk level of the data, such data may be subject to unauthorized access. For example, personnel data transferred to a management reporting system should have adequate controls to achieve the confidentiality and integrity objectives.

Establishing security and controls over report generation and distribution.

Controls over report generation and distribution should include the following:

- Reports should be reviewed for reasonableness and accuracy prior to distribution.
- Output distribution should be controlled so that output is provided to authorized recipients only and on a timely basis.
- Report retention should be adequate based on internal needs and regulatory requirements. For example, application output may be stored to back-up tapes (or kept as hard copy documentation) and rotated to an offsite storage facility.
- Output reports comply with applicable laws and regulations, including the type of clearance required to view the output reports.
- User access to reports is controlled based on the user's business need to view the report and the sensitivity of information contained in the report.
- Data output to management reporting or other copies of output files are adequately controlled.

Exposure Draft

Table 46. Control Techniques And Suggested Audit Procedures For Critical Element BP-3 Transaction data output is complete, accurate, valid, and confidential.

Control activity	Control Object.	Control techniques	Audit procedures
BP-3.1 Outputs are appropriately defined by the management (form, sensitivity of data, user selectivity, confidentiality, etc)	C,A,V,CF	<p>BP-3.1.1 Management has developed a reporting strategy that includes the following:</p> <ul style="list-style-type: none"> • content and availability that are consistent with end users' needs, • sensitivity and confidentiality of data • appropriate user access to output data. 	<p>Inquire of management about a reporting strategy or policy. Obtain a copy of any formal reporting strategy or policy.</p> <p>Assess the adequacy of the strategy and related policies.</p>
BP-3.2 Output generation and distribution are aligned with the reporting strategy.	C,A,V,CF	<p>BP-3.2.1 Management has procedures in place to reasonably assure that content and availability of output and data are consistent with end users' needs, sensitivity, laws and regulations, and confidentiality of data and valid user access.</p>	<p>Inspect management procedures for defining and assigning output/reports.</p> <p>Select key output/reports in the area of audit scope and verify the user access to the output/reports.</p>
		<p>BP-3.2.2 Management has procedures in place to monitor replication of output data used in management reports or other communications within or outside the entity.</p>	<p>Inquire of management on the use of data output. Inspect selected management reports or other communication to verify the accurate replication of data. Verify that the user received appropriate authorization to use the data.</p>
		<p>BP-3.2.3 User access to output data is aligned with the user's role and confidentiality/sensitivity of information.</p>	<p>Review user access to selected output data and assess the appropriateness of access.</p>
BP-3.3 System generated outputs/reports are reviewed to reasonably assure the integrity of production data and transaction processing.	C,A,V	<p>BP-3.3.1 Management has identified key reports to track processing results.</p>	<p>Inquire of user management and personnel to determine the key reports used to track processing results.</p>
		<p>BP-3.3.2 Management has documented procedures to review processed results, where applicable.</p>	<p>Obtain and inspect reports identified by management in the above test to determine whether the reports exist and are reviewed on a timely basis.</p>
		<p>BP-3.3.3 Procedures are in place to review critical output data or control reports on a timely basis.</p>	

Exposure Draft

Control activity	Control Object.	Control techniques	Audit procedures
BP-3.4 Output/ reports are in compliance with applicable laws and regulations.	C,A,V,CF	BP-3.4.1 Output reports for compliance with applicable laws and regulations are accurate, complete	Inspect a sample of output/reports for compliance with applicable laws and regulations. Identify laws and regulations that are to be complied with and verify that the reports are in compliance.
BP-3.5 Access to output/reports and output files is based on business need and is limited to authorized users.	CF	BP-3.5.1 Access to reports is restricted to those users with a legitimate business need for the information. BP-3.5.2 Users should have appropriate authorization for accessing reports, including the appropriate level of security clearance, where applicable.	Select output/reports and output files from the audit area and inspect application access (if the output can be accessed on-line or other electronic form) or inspect distribution to determine whether the user has appropriate level of security clearance and is authorized to access.

Source: GAO.

BP-4 Master Data Setup and Maintenance is Adequately Controlled

Master data are the key information that is constant and shared with multiple functions, such as a customer master record, which contains the customer number, shipping address, billing address, key contact and payment terms. Most applications use the following two types of master data:

Configurable master data or business rules are defined in an application module and used by end users, but cannot be changed directly in production. Purchase order release procedures (requiring approval) and payment terms are examples of business rules.

Business master data are master data created in production based upon the criteria designed to capture essential standing data, for example, customer and vendor master data.

Master data are, usually, entered once and are shared among various application modules. Also, common data fields that are used from origin may be used by the application several times over a period of time until the master data is no longer valid because of termination of a contractual agreement or data owner decision.

Exposure Draft

Three key control areas specific to master data controls are the controls related to design and configuration of master data (preventive), the procedures external to the system (detective and preventive), and the monitoring of master data design compliance (detective). Master data is also subject to access controls (activities to create and maintain master data are controlled by access privileges) discussed in AS-2.

The three key steps in master file setup and maintenance are:

- Implementing an effective design of master data elements
- Establishing master data maintenance procedures, including approval, review, and adequate support for changes to master data
- Implementing an effective auditing and monitoring capability

Implementing an effective design of master data elements

Master data elements should be designed to minimize the risk of erroneous master data. The effectiveness of master data design can be affected by the following:

- Centralized versus decentralized maintenance – centralized master data maintenance provides a greater control over creation and change of master data. It could, however, delay the process. Since most applications provide field or functional level access, it is possible for key data to be centrally maintained and functional specific data maintained by a unit. For example, vendor master data can be segmented into purchasing data and finance data, separately maintained by purchasing and finance departments, respectively.
- Partial edit – Master data maintenance may be controlled by rules that can be configured to prevent changes to certain areas of data, or key fields within a record.
- Numbering – System-assigned internal numbering is generally considered to be lower risk than external numbering, however, management can choose to use external numbering (to match numbers from an external system) and can choose naming

Exposure Draft

conventions appropriate to its use. Adequate procedures should be in place to reasonably assure compliance with management's policy on numbering/naming conventions.

- Ownership – Ownership should be clearly identified.

Establishing master data maintenance procedures, including approval, review, and adequate support for changes to master data

As discussed earlier, master data are much more static than transaction data, which may be created and updated on a daily basis by a wide range of users. Master data maintenance, therefore, should be the domain of fewer users than those responsible for updating transaction data.

Because Master Data serves as the basis for transaction processing, it is critical that controls exist over the integrity and quality of the data. An erroneous Master Data record will compromise the integrity of whatever transactions use the field values stored in the master data. Characteristics of erroneous master data elements include, but are not limited to, duplicate names, invalid records, duplicate addresses, improper address formats, incomplete or inaccurate address information, unpopulated data fields and other data formatting inconsistencies between the business rules and the data sets.

Because it is foundational in nature and may have a broad impact on transactional data, master data should be carefully controlled through reviews and approval by designated data owners. To reasonably assure an appropriate level of control, a combination of automated, preventive controls and manual, detective controls is recommended.

Controls over master data include controls related to:

- changes to the configuration of the master file,
- validity of all master file records,
- completeness and validity of master file data,
- consistency of master data among modules, and

Exposure Draft

- approval of changes to master file data.

Implementing an effective auditing and monitoring capability

As part of the control of master data, the organization should have an effective auditing and monitoring capability which allows changes to master data records to be recorded and reviewed where necessary. This monitoring may be done either as part of ongoing activities or through separate “master data audits”. In either case, the most important factor supporting the capability is that activity is properly captured and maintained by an automated logging mechanism.

Depending on the level of risk associated with the data, the type and frequency of monitoring may vary. Ideally, monitoring should be built into the normal, recurring responsibilities of the data owner. Because audits take place after the fact, problems often will be identified more quickly by ongoing monitoring routines.

Ongoing monitoring may include obtaining approval prior to changes, or verifying the accuracy of changes on a real-time basis.

For federal systems, NIST SP 800-53 includes the following controls related to master data setup and maintenance:

SI-9 Information Input Restrictions SI-10 Information Accuracy, Completeness, Validity, and Authenticity SI-11 Error Handling

Exposure Draft

Table 47. Control Techniques And Suggested Audit Procedures For Critical Element BP-4 Master Data Setup and Maintenance is Adequately Controlled

Control activity	Control techniques	Audit procedures
BP-4.1 Master data are appropriately designed.	BP-4.1.1 An entry is required in all key fields, such as address and account number.	Inspect master data configuration for required field values.
	BP-4.1.2 Null values or invalid values are not accepted in the required fields.	Observe user input of invalid values, or blank values, and note any exceptions.
	BP-4.1.3 For financial applications, account assignments (asset, liability, income and expense) are accurately defined.	Inspect master data configuration for account groups and assignments.
BP-4.2 Changes to master data configuration are appropriately controlled.	BP-4.2.1 Policies and procedures are established for master data configuration management, which include change rules that identify data fields that are excluded from changes (for example, master data number).	Review the master data policies and procedures for change management.
	BP-4.2.2 Changes to the master data design are approved by appropriate personnel	Inspect a sample of change requests and verify that appropriate approvals are obtained. Inspect master data configuration for change rules, if the rules are configured. If the change rules are automatic, then the user should be prevented from making unauthorized configuration changes.
	BP-4.2.3 Changes to the master data records should be limited to non-key fields.	Inspect a sample of master data change reports and verify that changes are limited to management-defined non-key fields.

Exposure Draft

Control activity	Control techniques	Audit procedures
BP-4.3 Only valid master records exist.	<p>BP-4.3.1 Master data is reviewed on a regular basis, duplicates are identified and removed or blocked, and unused data is identified and blocked.</p> <p>BP-4.3.2 Automatic application controls (duplicate checks, system warnings) are configured to prevent and/or identify potential duplicate master records.</p>	<p>Inquire of management regarding their master data review procedures.</p> <p>Inspect policies and procedures on master data review, including duplicate master data entry and resolution, and unused master records.</p> <p>Inspect evidence of the most recent management review and action.</p> <p>Inspect list of accounts/records blocked for posting or use.</p> <p>Inspect duplicate master record report and management's use of it.</p> <p>Inspect application configuration for automatic controls and determine whether the controls prevent erroneous processing or simply warn of potential errors.</p>

Exposure Draft

Control activity	Control techniques	Audit procedures
BP-4.4 Master data are complete and valid.	BP-4.4.1 Policies and procedures for master data maintenance are documented and include: <ul style="list-style-type: none">• approval requirements;• data quality criteria;• data owner;• supporting documents;• backup procedures in the event of a disaster or data corruption error;• Archival policies.	Inspect master data maintenance policies and procedures for appropriateness. Select a sample of master data created or changed, and inspect relevant documentation, noting appropriate approvals and compliance with policies and procedures.
	BP-4.4.2 The master data maintenance process includes a formal create/change request from the requestor and approval from the data owner.	Obtain system report of users with master data maintenance access. For a sample of users with conflicting responsibilities, inspect user profiles noting evidence of segregation of duty consideration and review when conflicts are noted.
	BP-4.4.3 Segregation of duties conflicts are considered and resolved before providing access to master data transactions.	Inquire of responsible personnel and inspect policies and procedures covering master data maintenance. Inspect procedures for identifying, segregation of duty exceptions, and review compliance.
	BP-4.4.4 Edit reports are reviewed by appropriate data owners on a periodic basis to review new master data and changes made to existing master data.	Inspect evidence of proper review of edit reports by owners
BP-4.5 Master data are consistent among modules.	BP-4.5.1 Periodic review and reconciliation procedures are in place to ensure that master data are consistent between different application modules.	Inspect evidence of management reconciliation and review for effectiveness. Through inquiry and inspection, determine whether the frequency of management reconciliation of master data is appropriate.

Exposure Draft

Control activity	Control techniques	Audit procedures
BP-4.6 Master data additions, deletions, and changes are properly managed and monitored by data owners.	BP-4.6.1 Master data policies and procedures require data owner's to be responsible for the creation, deletion, and change of master data and also changes to data characteristics.	Review policies and procedures and inquire of data owner concerning application of specific monitoring procedures.
	BP-4.6.2 Data owners monitor master data design changes, and approve and monitor creation, deletion and changes to master data on a regular basis.	Obtain and inspect evidence of monitoring by data owners, including related reports.
		Inquire of management regarding ongoing monitoring of master data changes.
		Obtain and inspect evidence of management review of master data design changes, and determine whether changes are approved and reviewed.
BP-4.7 As appropriate, the confidentiality of master data is adequately controlled	BP-4.7.1 Management implements adequate controls to protect the confidentiality of master data, as appropriate.	Assess the adequacy of management controls over confidentiality of master data.
		Coordinate this step with Critical Element AS-2 <i>Implement effective application access controls.</i>

Source: GAO.

Exposure Draft

4.3. Interface Controls (IN)

Interface controls consist of those controls over the a) timely, accurate, and complete processing of information between applications and other feeder and receiving systems on an on-going basis, and b) complete and accurate migration of clean data during conversion.

Interfaces⁹⁶ result in the structured exchange of data between two computer applications, referred to in this section as the source and target systems or applications. These applications may reside on the same or different computer systems that may or may not reside in the same physical environment. Interfaces are periodic and recurring in nature. Interface controls may be performed manually or automated, scheduled or event-driven, electronically or on paper. One interface transfers one business data object and is one-directional; e.g. vendor master outbound, sales order inbound, etc. Interfaces are never bi-directional, even if technically there may be handshaking, back-and-forth reconciliation, etc.

This section focuses on the scope of and controls for interfaces, governing specifically the extraction, transformation, and loading of data between two applications. The data input, validation, and output controls within an application are addressed in the preceding business process control sections.

The interface process, including conversions, can be broken down into the following seven separate components:

1. Interface strategy – A documented strategy is developed to keep data synchronized between source and target application. The strategy should include an explanation of each interface, the interface method chosen (manual or batch, etc.), the data fields being interfaced, the controls to reasonably assure that the data is interfaced completely and accurately, timing requirements,

⁹⁶In contrast, system interconnections refer to the direct connection of two or more IT systems for the purpose of sharing data and other information resources.

Exposure Draft

definition of responsibilities, on-going system balancing requirements, and security requirements.

2. **Data Export / Extraction** –The information needs of the target application (key information fields, ID fields and cross-reference fields) should be fully understood and documented. If the information needs are not fully understood, all relevant data may not be extracted. In addition, appropriate procedures/should be in place concerning the format, quality, cut-off, and audit trails related to source data.
 - a. The format of the source data should be checked to reasonably assure that the information is available, accurate and at the appropriate level of detail. If the source data quality is poor, the data may not be able to be interfaced.
 - b. Data processing should be cut-off as of a specific time to reasonably assure that the data is extracted for the proper period.
 - c. Sufficient audit trails should exist for the source application, such that once the data is extracted, the original audit trail remains. For instance, invoices can be traced back to the applicable purchase order in the source system.
3. **Data Mapping / Translation** – Data mapping and translation is the process of converting source data from the source application format to the target application format. If the data is not entered in the target application in exactly the same way as it is expected, target application edit and validation checks may be rendered ineffective.
4. **Data Import** – Data import is the process of loading source data into the target application. Appropriate controls, such as database indicies that enforce uniqueness, should be in place to prevent duplicate processing.
5. **Error Handling and Reconciliation procedures** – The procedures developed to reasonably assure that all transactions are

Exposure Draft

accounted for and that all errors are identified, isolated, analyzed, and corrected in a timely manner.

6. Job definition, Scheduling and Event Triggering – Due to business requirements, it may be necessary to initiate an interface daily, weekly, monthly, or after a triggering event. “Triggering events” are used to start interface processing based on specific criteria, such as date/time or completion of another event. Interfaces may run across multiple platforms. Therefore, interface jobs may need to be scheduled across platforms. Visibility of these jobs may be necessary in a single location by the system operators. Restart and recovery procedures should exist.
7. Data Handling – Interfaced data should be able to be retrieved to re-execute the interface, if needed. Controls should be established to support the confidentiality and proper handling of sensitive data. Access to interface data and processes should be properly restricted.

The objectives of interface controls are to:

- Implement an effective interface strategy and design
- Implement effective interface processing procedures, including
 - interfaces are processed completely, accurately and only once in the proper period.
 - interface errors are rejected, isolated and corrected in a timely manner.
 - access to interface data and processes are properly restricted. Data is reliable and obtained only from authorized sources

Exposure Draft

For federal systems, NIST SP 800-53 includes the following controls related to interface:

SI-9 Information Input Restrictions SI-10 Information Accuracy, Completeness, Validity, and Authenticity SI-11 Error Handling

Critical Elements

The critical elements for interface controls are:

IN-1 Implement an effective interface strategy and design IN-2 Implement effective interface processing procedures

Because weaknesses in interface controls can affect the achievement of all of the control objectives (completeness, accuracy, validity, and confidentiality) related to applications data, the control activities in the control tables for interface controls do not contain reference to specific control objectives.

Critical Element IN-1: Implement an effective interface strategy and design.

The purpose of an interface strategy is to describe, at a high level, how the interfaces are implemented between two applications. The interface strategy is the basis for the interface design and scope. The interface strategy includes an explanation of each interface, the interface method chosen (manual or batch, etc.), the data fields being interfaced, the controls to reasonably assure that the data is interfaced completely and accurately, timing requirements, assignment of responsibilities, on-going system balancing requirements, and security requirements. Interface design uses guidelines set by the strategy and provides specific information for each of the characteristics defined in the strategy.

Exposure Draft

Table 48. Control Techniques and Suggested Audit Procedures for Critical Element IN-1: Implement an effective interface strategy and design.

Control activities	Control techniques	Audit procedures
IN-1.1 An interface strategy is developed for each interface used in the application.	IN-1.1.1 An interface strategy exists for each interface that includes the interface method, data fields being interfaced, controls to reasonably ensure a complete and accurate interface, schedule, assignment of responsibilities, system balancing requirements and security requirements.	Obtain a list of all interfaces to and from the application audited. Inspect the interface strategy document noting the details of each interface and determine whether it contains appropriate information.
IN-1.2 An interface design is developed for each interface used in the application that includes appropriate detailed specifications.	IN-1.2.1 An interface design exists for each interface and includes appropriate specifications based on the business requirements, including: <ul style="list-style-type: none"> • validations and edits • ownership of the interface process • error correction and communication methods 	Inspect interface design documents of each interface and determine whether it contains appropriate information.
	IN-1.2.2 Mapping tables are used to convert data from the source system to the target system. Controls are in place to reasonably assure that mapping tables are only changed when authorized and that historical data on mappings is retained with the previous mapping table.	Determine whether the interfaces use mapping tables. Verify that controls over mapping tables will be established.
	IN-1.2.3 If mapping tables are not used, appropriate edits and validations are present in the source system.	Verify whether the appropriate edits and validations are implemented in the source systems.

Source: GAO.

Critical Element IN-2: Implement effective interface processing procedures

Because there may be several methods that are used to transfer data from one system to another, the auditor should understand the procedures that are used for each interface, including:

- Who is the owner of the interface? Who initiates the process?
- How is the data transferred from the source application?
- How often are the interface programs run?
- How does the target system get the notification of an interface?
- Where are the errors corrected - in the source or target system?

Controls surrounding interface processing should reasonably assure that data is transferred from the source system to target system completely, accurately, and timely. The processing routines should include balancing by ensuring the opening balance control totals plus processed transactions equal the closing balance of control totals. Both the applications (source and target) are typically

Exposure Draft

designed with controls so that data are controlled by the use of control totals, record counts, batching run totals, or other data logging techniques. These types of controls are commonly referred to as balancing controls. Records or data produced by one application may be used in another application and may have dependencies that are based upon the sequential processing of data. The entity should have effective procedures to reconcile control information between the source and target applications.

During interface processing, all data may not be processed completely or accurately as a result of errors or inconsistencies in data, system interruptions, communication failures, or other events. To identify these instances, a monitoring capability should be implemented. The objective of the monitoring function is to reasonably assure that data are accurately processed through the interface and that no data are added, lost, or altered during processing. Control techniques include:

- If the interface is “run” on a regular schedule to process data, either manually or automatically, documented procedures explain how this is performed, including controls in place to reasonably assure that all processing was completed.
- An interface processing log is maintained and reviewed for unusual or unauthorized activity.
- The interface processing log, or another log or report, is used to document any errors or problems encountered during processing. Types of information that should be considered for logging are descriptions of any errors encountered, dates identified, any codes associated with errors, any corrective action taken, date and times corrected.
- Procedures are in place to use the correct generation/cycle of files for processing. This may include the generation of backup files from processing to be used for disaster recovery.
- Audit trails are generated during processing. These audit trails should be logs or reports that contain information about each interface. Data that should be included are who initiated each of

Exposure Draft

the interfaces, the data and time of the run, the source system, and the results.

- Procedures are implemented to identify and correct any errors that occur during the interface run. Error handling procedures during data entry should reasonably assure that errors and irregularities are detected, reported, and corrected. Errors should be corrected in the source system and reprocessed through the next run. Management should have procedures in place to reasonably assure that error logs are used to timely follow-up on and correct unresolved data errors and irregularities.

Table 49. Control Techniques And Suggested Audit Procedures For Critical Element Critical Element Critical Element IN-2: Implement effective interface processing procedures.

Control activities	Control techniques	Audit procedures
IN-2.1 Procedures are in place to reasonably assure that the interfaces are processed accurately, completely and timely	IN-2.1.1 Procedures include a complete list of interfaces to be run, the timing of the interface processing, how it is processed and how it is reconciled. If system interconnections are used, procedures should address requirements for an Interconnection Security Agreement and Memorandum of Understanding.	Inspect documentation of interface processing procedures and, if applicable, Interconnection Service Agreements and Memorandums of Understanding.
	Timing for processing of the interface has been determined and is followed.	Observe interface processing into the application.
	A positive acknowledgement scheme is used to ensure that files sent from a source system are received by the target system (i.e., a "handshake" between the systems so that files are not skipped or lost).	Determine whether data and files from interface activities are processed according to the stated policies and in the proper accounting period.
IN-2.2 Ownership for interface processing is appropriately assigned.	IN-2.2.1 Responsibility for processing the interface and correcting any errors has been assigned to a user from the source and to a user of the target system. Actual processing may involve a technical person, if the interface is processed via an electronic media, such as a tape.	Determine whether all files sent from the source system are received and acknowledged by the target system.
	IN-2.2.2 The files generated by an application interface (both source and target) are properly secured from unauthorized access and/or modifications.	Identify which users are assigned responsibility for the interfaces. Evaluate whether an appropriate level of resources has been assigned to maintain interfaces.
		Assess whether appropriate security is in place for all access points to the interface data are secure from unauthorized use.
		Identify individuals that will be responsible for providing security surrounding the interfaces.

Exposure Draft

Control activities	Control techniques	Audit procedures
	IN-2.2.3 Users who are processing interfaces are able to monitor the status of interfaces.	Assess whether proper access is assigned to the appropriate individuals for the monitoring of the interface status and that such individuals have access to appropriate information to monitor the status of the interface.
IN-2.3 The interfaced data is reconciled between the source and target application to ensure that the data transfer is complete and accurate.	IN-2.3.1 Reconciliations are performed between source and target applications to ensure that the interface is complete and accurate. Control totals agree between the source and target systems. Reports reconcile data interfaced between the two systems and provide adequate information to reconcile each transaction processed.	Inspect reports or other documents used to reconcile interface processing between source and target applications and review their content and frequency for appropriateness.
IN-2.4 Errors during interface processing are identified by balancing processes and promptly investigated, corrected and resubmitted for processing.	IN-2.4.1 Management maintains a log for interface processing. The log accounts for errors and exceptions, as well. Exception/error reports are produced, reviewed, and resolved by management on a regular basis, including correction and resubmission, as appropriate.	Through inquiry of management and review of logs, determine whether errors are properly handled. Assess the appropriateness of the frequency that exception reports are reviewed (daily, weekly, etc). Inspect evidence of such reviews having been performed.
IN-2.5 Rejected interface data is isolated, analyzed and corrected in a timely manner.	IN-2.5.1 Error and correction facilities are utilized to track and correct errors in interface data.	Assess the adequacy of procedures in place to properly correct any rejected transactions. Inquire about procedures applied with individuals responsible for identifying and correcting errors and inspect evidence that rejected data is properly processed timely basis.
	IN-2.5.2 A mechanism is used to notify users when data is rejected (for example, an e-mail message may be sent to the user). These messages should repeat daily until they are corrected.	Determine whether error messages are generated and promptly reviewed for all rejected data and are maintained until corrected.
	IN-2.5.3 Audit trails are used to identify and follow-up on interface errors. The corrections to interface errors are included in the audit trail.	Determine whether appropriate audit trails are generated, reviewed and maintained.
IN-2.6 Data files are not processed more than once.	IN-2.6.1 Interfaces files are automatically archived or deleted from the production environment after processing.	Inspect a sample of archived interface documents and verify the date and time of processing. Observe the interfaces that are in process and inspect evidence that they were not processed before in the same period.

Source: GAO.

Exposure Draft

4.4 Data Management System Controls (DA)

Applications that support business processes typically generate, accumulate, process, store, communicate and display data. Applications which handle significant volumes of data often employ data management systems to perform certain data processing functions within an application. Data management systems use specialized software which may operate on specialized hardware. Data management systems include database management systems, specialized data transport/communications software (often called middleware), cryptography used in conjunction with data integrity controls, data warehouse software and data reporting/data extraction software. Many of the data input and processing controls, such as edit checks, existence checks and thresholds described in previous sections are implemented in functions of data management systems. These types of controls implemented in data management systems are often referred to as business rules.

When assessing the effectiveness of application controls, the auditor should evaluate functions of data management systems specific to the business processes under review, in addition to the general controls described in Chapter 3. When auditors are evaluating application security plans and independently assessing risk, consideration of the risk inherent to the data management system “layer” in the application architecture is important. Necessarily, multiple access paths must exist into the data and the business rules that reside in the data management system layer to facilitate the operation and administration of the application. In most large scale and/or high performance applications, various components of data management systems reside on different servers which often employ various operating systems and hardware technologies. The auditor should obtain an understanding of the interconnected combination of data management technologies and appropriately consider related risks.

Understanding the logical design and physical architecture of the data management components of the application is necessary for the auditor to adequately assess risk. In addition to supporting the data storage and retrieval functions, it is typical for applications to employ data management systems to support operational aspects of

Exposure Draft

the application, such as the management of transient user session state data, session specific security information, transactional audit logs and other “behind the scenes” functions that are essential to the application’s operation. Controls associated with these types of functions can be critical to the security of the application.

The following highlights certain key concepts the auditor considers when assessing controls over a data management systems, including database management systems, middleware, cryptography, data warehouse, and data reporting/data extraction software.

Key Concepts - Database Management Systems

Authentication/Authorization

Controls in a data management system should include consideration of the access paths to the data management system. The access paths should be clearly documented and updated as changes are made. Generally access to a data management system can be obtained in three ways, via:

- Directly, via the database management system;
- Through access paths facilitated by the application; or
- Through the operating system(s) underlying the database management system.

Data management systems have built in privileged accounts that are used to administer and maintain the data management system. The auditor's objective is to determine whether appropriate controls are in place for securing these privileged accounts. Such controls include, but are not limited to:

- Strong password usage or other authentication controls;
- Highly restrictive assignment of personnel to these accounts;
- Enforcement of unique accounts for each administrator; and
- Effective monitoring of privileged account use.

Exposure Draft

In addition to privileged accounts, the auditor should obtain an understanding of the role the data management system plays in authentication and authorization for the application. The data management system will also contain user accounts related to the application.

Generally, there are two methods of authentication using a data management system. In the first scenario, the application uses a generic ID to authenticate to the database on behalf of end-users. These generic IDs should have their access privileges carefully scoped to only provide access to what the highest level of end-user is permitted to access. There should be a limited number of generic IDs within the database supported by well-documented and carefully monitored control procedures. In the second scenario, the application passes the user ID to the database and uses accounts assigned to each end-user to authenticate to the database. Depending upon the size of the application, there could be a large number of user accounts stored within the database management system. In either case, the auditor should review the account and password policies relevant to the database management system.

There may be situations where authentication to the data management system is done through the operating system. The auditor should, in such instances, coordinate testing of general controls related to the operating system.

There are two major types of database management systems in use, hierarchical and relational databases. Hierarchical databases, such as IBM's IMS, have a heritage near the beginning of computer systems; however they are still used in some modern applications. Each different hierarchical database product is proprietary in design and implementation. If achieving audit objectives involving hierarchical databases is a requirement, staff with knowledge of the specific database product will be necessary. Relational databases (such as Oracle, DB2, and SQL-Server) share a common design based on relational algebra and a common data access method, called the Structured Query Language (SQL). While there are differences in the implementation of the different relational database products, they are similar enough that staff should be able to perform audit work in most relational database systems with a

Exposure Draft

common skill set. The discussion in this chapter will focus on relational database systems.

SQL Commands

There are two categories of commands available through SQL, data definition language statements (DDL) and data manipulation language statements (DML). DDL statements are used to define and alter the structures or objects that contain and support access to data. DDL statements are used to create, alter and delete objects such as tables and indices. DML statements are used to retrieve, add, change and delete data in existing database objects. Application end-users would not typically need to use DDL statements.

System, Role, Object Privileges

A user *privilege* is a right to execute a particular type of Structured Query Language (SQL) server statement, or a right to access another user's object. As discussed below, there are two types of data management system privileges: system and object. *Roles* are created by users (usually administrators), and are used to group together privileges or other roles. They are a means of facilitating the granting of multiple privileges or roles to users.

System privileges relate to the ability of the user within the database to interact with the database itself **using DDL statements and the ability to execute special functions**. They include: CREATE, ALTER, DROP, CONNECT, and AUDIT, among many others. The auditor should examine the privileges granted to the users within the database. Typically administrator level accounts have extended system privileges while general user accounts should have limited access to system privileges.

Object privileges (through DML statements) allow the user to have access to the data within an object or allow the user to execute a stored program. These include SELECT, INSERT, DELETE, etc. Each type of object has different privileges associated with it. Examples of database objects include the following:

Exposure Draft

- **Tables** - A data structure containing a collection of rows (or records) that have associated columns (or fields). It is the logical equivalent of a database file.
- **Index** - A database object that provides access to data in the rows of a table, based on key values. Indexes provide quick access to data and can enforce uniqueness on the rows in a table.
- **Triggers** - A special form of a stored procedure that is carried out automatically when data in a specified table is modified. Triggers are often created to enforce referential integrity or consistency among logically related data in different tables.
- **Stored procedure** – A precompiled collection of SQL or other statements and optional control-of-flow statements stored under a name and processed as a unit. Stored procedures are stored within a database, can be executed with one call from an application, and enable user-declared variables, conditional execution, and other powerful programming features.
- **Views** - A virtual table generated by a query whose definition is stored in the database. For example, a view might be defined as containing three out of five available columns in a table, created to limit access to certain information. Views can be treated as tables for most database operations, including Select queries, and under some circumstances, Update, Insert, and Delete queries. Any operations performed on views actually affect the data in the table or tables on which the view is based.

The auditor should identify the objects within the data management system. The privileges that a user account has for each object should be reviewed. These privileges should be granted based on the functionality of the account.

A *role* groups several privileges and roles, so that they can be granted to and revoked from users simultaneously. A role should be enabled for a user before it can be used by the user. Predefined roles exist that can be leveraged, such as the data base administrator (e.g., DBA) role. The auditor should review the privileges granted to each role, and then analyze the role(s) granted

Exposure Draft

to each user. Roles that grant high level access, or permit direct manipulation of data in the database are very sensitive. The auditor should evaluate controls over the use of such roles.

Stored Procedures

Stored procedures are programs that are compiled and stored in the data management system. These programs can be executed directly by a user or they can be called by other programs. Most data management systems are prepackaged with stored procedures that provide a structured and controlled method of administering the database. For example, when the administrator creates a user, the database management system uses a stored procedure to perform the steps necessary to create that account. In addition custom stored procedures can be created to support additional functionality. The auditor should review stored procedures that interact with sensitive data within the database management system or provide access to the operating system.

Key Concepts – Middleware

Modern business applications frequently have user interface, data processing and data storage components hosted on different computer systems, often using different operating systems. Tying the components together is often accomplished through the use of specialized data transport/communications software commonly known as middleware. A popular example of this type of software is IBM's MQSeries. Middleware is used to connect applications together in varying architectures including interconnected systems and interfaced systems (as described in 4.3).

Middleware provides robust and potentially secure communications between application components through layers of functions across a series of host computer and network technologies. In modern application architectures, the “behind the scenes” processing and storage of information may be designed to *trust* upstream application components, such as user interfaces, due to the data security and data integrity services provided by the middleware. Middleware can be used to communicate both data and commands

Exposure Draft

between systems using different operating systems. The communication links are often facilitated by *channels* created by the middleware. The channels can be configured so that they provide data security for the information flowing across the network, typically using cryptography, and data integrity through error detection and correction facilities. Middleware can also be an important aspect of an application's continuity of operations, by being configured to support multiple data paths to eliminate single points of failure across networks.

Middleware Controls

Middleware components can be found on many components in a network of computers used to support business applications. The location and function of these components should be well documented. Middleware carries not only data and system commands; it also typically facilitates the establishment of sessions between application components, often some level of application component logging onto a "back-end" host and database management system. An application's controls often rely on the encrypted transmission of information between components. This protection may be a function of the implementation of middleware, sometimes in conjunction with how the channels are configured across the network. As with other data management systems, auditors should identify the staff with administrative access privileges to middleware and verify that appropriate controls are in place.

Key Concepts – Cryptography

Modern business applications commonly employ one or more controls that rely on cryptographic services. Auditors should identify where these controls are deployed and verify that the technical implementations are appropriate and effective operational procedures are in place and being followed. The mere existence of cryptography provides no assurance that data controls are actually in place and effective. Due to the exacting nature of verifying the

Exposure Draft

effectiveness of cryptographic controls, a detailed discussion is beyond the scope of this audit guidance. When it is necessary to evaluate the effectiveness of cryptographic controls to achieve audit objectives, the auditor should obtain the services of adequately qualified specialists.

Key Concepts – Data Warehouse, Data Reporting and Data Extraction Software

Increasingly, modern business applications are parts of larger business management information architectures. This is certainly the case with ERP environments, but also is the result of interconnected and interfaced systems that supply information used for purposes beyond the application's primary business function. A common element in these combined business management information architectures is the data warehouse, which may be populated with both financial and non-financial business information. The data warehouse is often a separate data store, not operationally part of the entity's transactional systems. The reasons behind having this separate copy of business information can be multifold: separating the information eliminates potential performance issues associated with trying to use live transactional data for reporting; also the structure of the information in diverse business applications may be technically or logically incompatible with efficient information retrieval. When the auditor encounters a data warehouse, important questions related to audit objectives and system boundaries need to be addressed. Unless the data warehouse itself is the subject of the audit, the relevance to the audit objectives and potential risks created by the data warehouse need to be identified and evaluated. Since a data warehouse may represent a copy of information from other systems that are part of the audit, any data confidentiality concerns will likely need consideration. Additionally, the auditor may need to functionally understand how the entity uses the data warehouse. In a financial audit, the auditor may find that financial statements may be prepared, in part, from the data warehouse instead of directly from the general ledger.

Exposure Draft

A data warehouse typically exists to facilitate analysis and reporting from a large quantity of data. Supporting the efficient use of a data warehouse will often be specialized data reporting and data extraction software tools. The existence of these tools and data warehouses creates the potential for many different access paths to data. Depending on the control requirements of the data warehouse and the information it stores, the auditor may need to identify controls over how the data is populated, maintained, and accessed by both users and administrators. The software systems involved are often specialized and effective reviews may require the services of qualified specialists.

Segregation of Duties

Since data management systems are supported by one or more operating systems, the auditor should obtain an understanding of the role of the data management system administrators. There should be a distinct segregation between the data management system administrator and the operating system administrator. The operating system administrator may need access to the data management system, but should have limited access. Likewise, the data management system administrator may need access to the underlying operating system, but should have only the access necessary to manage the data management system functionality.

The auditor should also evaluate the segregation between the data management system administrator and personnel in charge of reviewing audit and transaction logs. The data management system administrator should not have access to the audit logs within the data management system. These logs should be reviewed by a security administrator.

There should also be a separation between the functional aspects of the data management system environments. Data management system access should be consistent with the functional separation of duties within the application environment. Users that are developers should have access to the development environment only, and consequently only the development data management system. Users that require access to production should only have access to the production data management system.

Exposure Draft

Control Activities

Control activities for data management system controls are:

DA-1.1 Implement an effective data management system strategy
 DA-1.2 Identify and respond to specific system or user security events within the data management system and its related components.
 DA-1.3 Properly control specialized data management processes.

Because weaknesses in data management controls can affect the achievement of all of the control objectives (completeness, accuracy, validity, and confidentiality) related to applications data, the control activities in the control tables for interface controls do not contain reference to specific control objectives.

Table 50. Control Techniques and Suggested Audit Procedures for Critical Element DA-1 - Implement an effective data management system strategy and design

Control activities	Control techniques	Audit procedures
DA-1.1 Implement an effective data management system strategy and design, consistent with the control requirements of the application and data. The strategy addresses key concepts including: <ul style="list-style-type: none"> ● database management, ● middleware, ● cryptography, ● data warehouse, and ● data reporting/data extraction. 	DA-1.1.1 The physical and logical (in terms of connectivity) location of the data storage and retrieval functions are appropriate.	Inspect documentation of the design of the data management system(s) associated with the application.
	DA-1.1.2 The production data management system is effectively separated from non-production systems (such as testing and development) and other production systems with lesser control requirements.	Assess whether the data management system is properly designed. Determine whether the design is properly implemented.
	DA-1.1.3 The database schema is consistent with access control requirements such that the organization of data and database-hosted functions correspond to the access limitations that need to be imposed on different groups of users.	Verify that all access paths to data and sensitive data management system administrative functions have been identified and are adequately controlled.
DA-1.2 Detective controls are implemented in a manner that effectively supports requirements to identify and react to specific system or user activity within the data management system and its related components.	DA-1.2.1 Logging and monitoring controls are in place at the data management system level which effectively satisfy requirements to accurately identify historical system activity and data access	Identify the security events that are logged and determine whether logging is adequate. Assess the adequacy of controls to monitor the audit logs.
	DA-1.2.2 Real-time or near real-time controls are in place to detect abnormal activity and security events	Assess the adequacy of controls to detect abnormal activity.

Exposure Draft

Control activities	Control techniques	Audit procedures
DA-1.3 Control of specialized data management processes used to facilitate interoperability between applications and/or functions not integrated into the applications (such as ad-hoc reporting) are consistent with control requirements for the application, data and other systems that may be affected.	DA-1.3.1 Data accuracy and completeness controls are in place and effective to correct and/or detect data anomalies. DA-1.3.2 The configuration of system connectivity that facilitates application to application and application to non-integrated functions is controlled to limit access appropriately.	Identify and obtain an understanding of specialized data management processes used to facilitate interoperability. Understand how system interconnectivity is controlled with respect to data management systems. Assess the adequacy of controls over specialized management processes. Note: These procedures should be closely coordinated with tests of general controls related to the data management systems.

Source: GAO.

Exposure Draft

Appendix I - Information System Controls Audit Planning Checklist

The auditor should obtain and document a preliminary understanding of the design of the entity's information system (IS) controls, including

- Understanding the entity's operations and key business processes,
- Obtaining a general understanding of the structure of the entity's networks
- Obtaining a preliminary understanding of IS controls.

In addition to this checklist, the auditor should obtain information from relevant reports and other documents concerning IS that are issued by or about the entity.

To facilitate this process, the following checklist has been developed as a guide for the auditor to collect preliminary information from the entity at the start of the audit. This checklist is intended as a starting point for collecting relevant IS control information. The information request can be tailored to the type of audit being performed. For example, an audit of application controls could be limited to the information needs listed in Sections I, II, and IV. The extent of the information requested from the entity will vary depending on whether this is a first year or follow-up review of IS controls. Also, as a result of the auditor's initial review and analysis of the information collected in this process, additional detailed information may need to be subsequently requested from the entity. The checklist is organized to request information on the entity's:

- organization and key systems/applications,
- prior audit reports/documents,
- IS general controls, and
- IS business process application level controls.

Exposure Draft

I. Organization and Key Systems/Applications

Understanding the entity's organization is a key to planning and performing the audit in accordance with applicable audit standards and requirements. Further, it helps to identify, respond to, and resolve problems early in the audit. Relevant information includes organizational structure, locations, use of contractors, key applications and IS platforms used to support them.

Document	Workpaper Reference
1. Entity's overall organizational chart with functional description of key components.	
2. Organizational charts that include functional description for security and IT components. Note: It is critical that the organizational relationships between management, information security, physical security, and computer operations are discernable.	
3. Name and functional description of relevant major applications, including functional owner, operating platform (including locations), operating system and version, and database management system and version. Note: FISMA requires agencies to maintain an inventory of all major systems.	
4. Name and functional description of relevant operating environments (e.g., general support systems (GSS)), including locations.	

Exposure Draft

Document	Workpaper Reference
5. List of contractors/third parties or other governmental entities that process information and/or operate systems for or on behalf of the entity.	
6. Significant changes in the IT environment or significant applications implemented within the recent past (e.g., within 2 years) or planned within the near future (e.g., 2 years)	

II. Prior Audit Reports/Documents

The auditor generally gathers planning information through different methods, including previous audits, management reviews, and other documents. These reports often provide invaluable information on the effectiveness of IS controls and provides clues to areas of particular risk. Of specific interest are those reports/documents dealing with the IS control environment, including GSS and major applications. Relevant information in this area includes the following.

Document	Workpaper Reference
1. Internal or third party information system reviews, audits, or specialized testing (e.g., penetration tests, disaster recovery testing) performed during the last 2 years (e.g., IG, GAO, SAS 70 reports).	
2. The entity's prior FISMA or equivalent entity reports on IS.	

Exposure Draft

Document	Workpaper Reference
3. The entity's annual performance and accountability report or equivalent reports (e.g., reports prepared under the Federal Financial Management Improvement Act of 1996, Federal Managers Financial Integrity Act of 1982, Government Management and Reform Act and Accountability of Tax Dollars Act of 2002).	
4. Other reports by management, including privacy impact assessments and vulnerability assessments.	
5. Consultant reports on IS controls.	

III. IS General Controls

General controls are the policies and procedures that apply to all or a large segment of an agency's information systems and help ensure their proper operation. General controls are applied at the entitywide, system, and business process application levels. The effectiveness of general controls at the entitywide and system levels is a significant factor in determining the effectiveness of business process application controls at the application level. General controls include security management, access controls, configuration management, segregation of duties, and contingency planning.

III.1 IS General Controls – Security Management

Security management provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the agency's computer-related controls. The program should reflect the agency's consideration of the following critical elements for security management – established security management program, periodic

Exposure Draft

risk assessments, documented security policies and procedures, established security awareness training, and periodic management testing and evaluation of major systems. Other elements include implementing effective security-related personnel policies and ensuring that activities performed by external third parties are adequately secure. Relevant information for this control category includes the following.

Document	Workpaper Reference
1. Documentation of entity's security management program approved by OMB.	
2. Documented risk assessments for relevant systems (e.g., GSS and major applications).	
3. Certification and accreditation documentation or equivalent for relevant systems (e.g., GSS and major applications being reviewed).	
4. Documented security plans for relevant systems (e.g., GSS and major applications being reviewed).	
5. Agency performance measures and compliance metrics for monitoring the security processes.	
6. Management's plans of actions and milestones or their equivalent, that identify corrective actions planned to address known IS weaknesses and status of prior year security findings.	

Exposure Draft

Document	Workpaper Reference
<p>7. Entitywide policies and procedures governing</p> <ul style="list-style-type: none">• security management program, structure, and responsibilities, including system inventories• risk assessment• security awareness training for employees, contractors, third parties (including those in sensitive security and data processing position) and security-related personnel policies (including personnel hiring, reference and background checks, and job transfers and terminations),• performance of periodic tests and evaluations of IS controls and monitoring to ensure compliance with established policies and procedures (including copies of tests and evaluations performed (if not included under Section II “Prior Audit Reports/ Documents”),• security weakness remediation, and• security requirements and monitoring activities of third-party providers supporting specific application(s).	

III.2 IS General Controls – Access Controls

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Organizations accomplish this objective by designing and implementing controls that are intended to prevent, limit, and detect

Exposure Draft

unauthorized access to computing resources, programs, information, and facilities. Inadequate access controls diminish the reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and disruption of service. Access controls include those related to protecting system boundaries, user identification and authentication, authorization, protecting sensitive system resources, audit and monitoring, and physical security. Relevant information for this control category includes the following.

Document	Workpaper Reference
<ol style="list-style-type: none">1. High-level network schematic which identifies external network connections, inter- and intra-agency connections, contractor sites, and other external organizations. 2. Network schematic of all GSS (by site) that includes components such as:<ul style="list-style-type: none">• internet presence,• firewalls, routers, and switches,• domain name servers,• intrusion detection systems,• critical systems, such as web and email servers, file transfer systems, etc.• network management systems• connectivity with other entity sites and other external organizations• remote access – virtual private networks and dial-in, and• wireless connections.	

Exposure Draft

Document	Workpaper Reference
<p>3. Inventory of mid-level systems (Unix, Windows-based, etc.) supporting applications relevant to the audit.</p> <ul style="list-style-type: none">• operating systems/versions,• security software/versions,• list of systems/applications supported, and• data set naming conventions for the operating system, system configuration, utility software, applications, and security software.• documentation of basic security configuration settings, i.e. Windows-based, Unix, etc. <p>4. Inventory of mainframe systems including</p> <ul style="list-style-type: none">• operating systems/versions,• security software/versions,• IP addresses,• description and use of each LPAR configuration(production & non production),including list of user applications and software installed on each LPAR and description of any test or development activity in each LPAR.• data set naming conventions for the operating system, system configuration, utility software, applications, and security software,• identity of Exits and SVCs, including load library and module name, and• documentation of basic security configuration settings, i.e. RACF, Top Secret, or ACF2.	

Exposure Draft

Document	Workpaper Reference
<p>5. Entitywide policies and procedures for</p> <ul style="list-style-type: none">• system boundaries• controlling remote access to agency information, including use of remote devices,• governing user and system identification and authentication,• requesting, approving, and periodically reviewing user access authorization,• restricting access to sensitive system resources (including system utilities, system software, and privileged accounts),• protecting digital and sensitive media, including portable media,• applying cryptography methods, if used,• monitoring mainframe, mid-level servers, and network systems for incidents, including management response and reporting on unusual activities, intrusion attempts, and actual intrusions, and• controlling physical security, including those concerning the granting and controlling of physical access to the data center and other IT sensitive areas. <p>6. Physical diagram of computer network and data center and other sensitive IT areas.</p>	

Exposure Draft

III.3 IS General Controls – Configuration Management

Configuration management involves the identification and management of security features for all hardware and software components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. By implementing configuration management, organizations can ensure that only authorized applications and software programs are placed into production through establishing and maintaining baseline configurations and monitoring changes to these configurations. Configuration management includes

- overall policies and procedures,
- maintaining current configurations,
- authorizing, testing, and approving configuration changes,
- monitoring the configuration, updating software on a timely basis, and
- documenting and controlling emergency changes.

Relevant information for this control category includes the following.

Document	Workpaper Reference
<p>1. Entitywide policies and procedures for:</p> <ul style="list-style-type: none">• configuration management, including the approval and testing of scheduled and emergency changes, and monitoring procedures to ensure compliance,• maintaining current configuration information,• authorizing, testing, approving, and tracking all configuration changes,• monitoring/auditing the configuration,	

Exposure Draft

Document	Workpaper Reference
<ul style="list-style-type: none">• patch management, vulnerability scanning, virus protection, emerging threats, and user installed software, and• emergency changes. <ol style="list-style-type: none">2. Copy of System Development Life Cycle Methodology (SDLC).3. Technical configuration standards for workstations, servers, related network components, mobile devices, mainframes, operating systems, and security software.4. Description of configuration management software.	

III.4 IS General Controls- Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structures that help ensure that no single individual can independently control all key aspects of a process or computer-related operation and thereby gain unauthorized access to assets or records. Often, organizations achieve segregation of duties by dividing responsibilities among two or more individuals or organizational groups. This diminishes the likelihood that errors and wrongful acts will go undetected, because the activities of one individual or group will serve as a check on the activities of the other. Effective segregation of duties includes segregating incompatible duties, maintaining formal operating procedures, supervision, and review. Relevant information for this control category includes the following.

Exposure Draft

Document	Workpaper Reference
<ol style="list-style-type: none">1. Entitywide policies and procedures for<ul style="list-style-type: none">• segregating duties.• periodically reviewing access authorizations.2. Management reviews conducted to determine that control techniques for segregating incompatible duties are functioning as intended.	

III.5 IS General Controls – Contingency Planning

Contingency planning is critical to ensuring that when unexpected events occur, key operations continue without interruption or are promptly resumed and that critical and sensitive data are protected. Critical elements for contingency planning include: assessing the critical and sensitive computer activities and identifying supporting resources, taking steps to minimize damage and interruption, developing and documenting a comprehensive contingency plan, and periodically testing the contingency plan and adjusting it as needed. Relevant information for this control category includes the following.

Document	Workpaper Reference
<ol style="list-style-type: none">1. Entitywide policies and procedures for:<ul style="list-style-type: none">• assessing the availability needs of entity systems,• backing-up data, programs, and software, and	

Exposure Draft

Document	Workpaper Reference
<ul style="list-style-type: none">• environmental controls, including emergency power, fire/smoke detection and response, hardware maintenance and problem management, alternate work sites, etc. <ol style="list-style-type: none">2. Documented contingency plan(s) and recent test results.	

IV. IS Business Process Application Level Controls

Business process application level controls are those controls over the completeness, accuracy, validity and confidentiality of transactions and data during application processing. The effectiveness of application level controls is dependent on the effectiveness of entitywide and system level general controls. Weaknesses in entitywide and system level general controls can result in unauthorized changes to business process applications and data that can circumvent or impair the effectiveness of application level controls. Application level controls are divided into the following four areas: application level general controls, business process controls, interface controls, and data management system controls. Relevant application specific information for this control category includes the following.

Document	Workpaper Reference
<ol style="list-style-type: none">1. Certification and accreditation, or equivalent, documentation for relevant systems.2. Documented security plans for relevant applications.3. Documented risk assessments for relevant applications.	

Exposure Draft

Document	Workpaper Reference
<p>4. High-level schematic of application boundaries that identifies controlled interfaces (e.g., gateways, routers, firewalls, encryption), to include:</p> <ul style="list-style-type: none">• internet presence,• firewalls, routers, and switches,• domain name servers,• intrusion detection systems,• critical systems, such as web and email servers, file transfer systems, etc.• network management systems• connectivity with other entity sites and other external organizations• remote access – virtual private networks and dial-in, and <p>5. Inventory of mid-level systems (Unix, Windows, etc.) supporting applications being reviewed.</p> <ul style="list-style-type: none">• operating systems/versions,• security software/versions,• list of systems/applications supported,• data set naming conventions for the operating system, system configuration, utility software, applications, and security software, and• documentation of basic security configuration settings, i.e. Windows-based, Unix.	

Exposure Draft

Document	Workpaper Reference
<p>6. Inventory of mainframe systems supporting applications being reviewed, including</p> <ul style="list-style-type: none">• operating system/versions,• security software/versions,• IP addresses,• description of each LPAR configuration, including list of user applications and software installed on each LPAR,• data set naming conventions for the operating system, system configuration, utility software, applications, and security software,• identity of Exits and SVCs, including load library and module name.• documentation of basic security configuration settings, i.e. RACF, Top Secret, or ACF2.	
<p>7. Documented test and evaluation covering relevant applications.</p>	
<p>8. Corrective action plan for identified IS application control weaknesses, including listing of weaknesses corrected.</p>	
<p>9. Segregation of duties control matrices for job functions/responsibilities.</p>	
<p>10. Application contingency plan and related disaster recovery, business continuity, and business resumption plans, including test results.</p>	
<p>11. Documentation on data validation and edit checks, including auditing and monitoring processes.</p>	

Exposure Draft

Document	Workpaper Reference
12. Documentation describing interface strategy between applications, including both manual and automated methods.	
13. Documentation describing data management system used, including access paths to this system, privileged accounts, and authentication and authorization processes.	
14. Policies and procedures for relevant application(s) being reviewed that govern <ul style="list-style-type: none">• operation of application controls,• security and awareness training for employees and contractors,• granting user application access,• hiring, including reference and background checks, and job transfers and terminations,• security requirements and monitoring activities of third-party providers supporting relevant applications.• application user identification and authentication at the application level,• requesting and granting user access authorization to relevant applications,• collection, review, and analysis of access activities for unauthorized or inappropriate access to relevant applications,	

Exposure Draft

Document	Workpaper Reference
<ul style="list-style-type: none">• configuration management process at the application level, including the approval and testing of scheduled and emergency application program changes and procedures to ensure compliance,• backing-up relevant application data and programs,• approval and review of data input, and• master file data configuration management and maintenance.	
15. Documentation describing system output, format of the output, and controls over the output.	

Exposure Draft

Appendix II - Tables for Summarizing Work Performed in Evaluating and Testing General and Business Process Application Controls

These tables are provided for the auditor's use in performing the audit. They are a consolidation of the tables of critical elements, control activities, control techniques, and related suggested audit procedures that are included after the discussion of each critical element. To reduce documentation and allow the tables to be tailored to individual audits, the tables will be available in electronic form from GAO's World Wide Web server when the final FISCAM is issued. Our Internet address is: <<http://www.gao.gov>>.

These tables can be used as a guide during initial interviews and to document the preliminary assessment of controls. As the audit progresses, the auditor can continue to use the electronic version of the tables to document controls evaluated and tested, test procedures performed, conclusions, and supporting work paper references.

Note: For purposes of the Exposure Draft, only the first page is to provide for illustration. The table will ultimately be populated with the information in the Control Techniques and Suggested Audit Procedures tables in Chapters 3 and 4.

Exposure Draft

General Controls

Table 3. Security Management

Critical element and control activity	Control technique	Audit procedure	Entitywide level conclusion/reference	System level conclusion/reference	Application level conclusion/reference	Overall conclusion/reference
SM-1. A security management program has been established	<p>SM-1.1.1. An entitywide security management program has been developed, documented, and implemented. It covers all major facilities and operations, has been approved by senior management and key affected parties, covers the key elements of a security management program:</p> <ul style="list-style-type: none"> • periodic risk assessments • adequate policies and procedures • appropriate subordinate information security plans • security awareness training • management testing and evaluation • remedial action process 	<p>Review documentation supporting the entitywide security management program and discuss with key information security management and staff.</p> <p>Determine whether the program:</p> <ul style="list-style-type: none"> • adequately covers the key elements of a security management program • is adequately documented, and • has been properly approved. <p>Determine whether all key elements of the program are implemented.</p> <p>Consider audit evidence obtained during the course of the audit.</p>				

Exposure Draft

Appendix III - Tables for Assessing the Effectiveness of General and Business Process Application Controls

The tables in this appendix are provided for the auditor's use in recording the control effectiveness for each critical element in each control category, as well as formulating an overall assessment of each control category. Judging control effectiveness should be based on the results of audit work performed and assessments of control effectiveness for specific control techniques, as summarized in Appendix II. After completing Appendix III, the auditor should prepare a narrative summarizing the control effectiveness for general and business process controls. The general control narrative should also state whether or not audit work should be conducted to determine the reliability of business process controls at the application level. To reduce documentation and allow the tables to be tailored to individual audits, the tables will be available in electronic form from GAO's World Wide Web server when the final FISCAM is issued. Our Internet address is: <http://www.gao.gov>.

General Controls

Security Management

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
SM-1. Establish a security management program					
SM-2. Periodically assess and validate risks					
SM-3. Document security control policies and procedures					
SM-4. Implement effective security awareness of other security-related personnel policies					

Exposure Draft

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
SM-5. Monitor the effectiveness of the security program					
SM-6. Effectively remediate information security weaknesses					
SM-7. Ensure that activities performed by external third parties are adequately secure					
Overall assessment of security management					

Access Control

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
AC-1. Adequately protect information system boundaries					
AC-2. Implement effective identification and authentication mechanisms					
AC-3. Implement effective authorization controls					
AC-4. Adequately protect sensitive system resources					
AC-5. Implement an effective audit and monitoring capability					
AC-6. Establish adequate physical security controls					
Overall assessment of access controls					

Exposure Draft

Configuration Management

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
CM-1. Develop and document CM policies, plans, and procedures					
CM-2. Maintain current configuration identification information					
CM-3. Properly authorize, test, approve, and track all configuration changes					
CM-4. Routinely monitor the configuration					
CM-5. Update the software on a timely basis to protect against known vulnerabilities					
CM-6. Appropriately document and approve emergency changes to the configuration					
Overall assessment of configuration management					

Segregation of Duties

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
SD-1. Segregate incompatible duties and establish related policies					
SD-2. Control personnel activities through formal operating procedures, supervision, and review					
Overall assessment of segregation of duties					

Exposure Draft

Contingency Planning

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
CP-1. Assess the criticality and sensitivity of computerized operations and identify supporting resources					
CP-2. Take steps to prevent and minimize potential damage and interruption					
CP-3. Develop and document a comprehensive contingency plan					
CP-4. Periodically test the contingency plan and adjust it as appropriate					
Overall assessment of contingency planning					

Exposure Draft

Business Process Application Level Controls

Application Level General Controls

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
AS-1. Implement effective application security management					
AS-1.1. Establish an application security plan					
AS-1.2. Periodically assess and validate application security risks					
AS-1.3. Document and implement application security policies and procedures					
AS-1.4. Implement effective security awareness and other security-related personnel policies					
AS-1.5. Monitor the effectiveness of the security program					
AS-1.6. Effectively remediate information security weaknesses					
AS-1.7. Implement effective security-related personnel policies					
AS-1.8. Adequately secure, document, and monitor external third party activities					
Overall assessment of application security management					
AS-2. Implement effective application access controls					
AS-2.1. Adequately protect application boundaries					
AS-2.2. Implement effective identification and authentication mechanisms					
AS-2.3. Implement effective authorization controls					
AS-2.4. Adequately protect sensitive system resources					
AS-2.5. Implement an effective access audit and monitoring capability					
AS-2.6. Establish adequate physical security controls					
Overall assessment of access controls					
AS-3. Implement effective configuration management					
AS-3.1. Develop and document CM policies, plans, and procedures					
AS-3.2. Maintain current configuration identification information					
AS-3.3. Properly authorize, test, approve, and track all configuration changes					
AS-3.4. Routinely monitor the configuration					
AS-3.5. Update systems in a timely manner to protect against known vulnerabilities					
AS-3.6. Appropriately document and approve emergency changes to the configuration					
Overall assessment of configuration management					
AS-4. Segregate user access to conflicting transactions and activities and monitor segregation					

Exposure Draft

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
AS-4.1. Segregate user access to conflicting transactions and activities					
AS-4.2. Monitor user access to conflicting transactions and activities through formal operating procedures, supervision, and review					
Overall assessment of segregation of duties					
AS -5. Implement effective application contingency planning					
AS-5.1. Assess the criticality and sensitivity of computerized operations and identify supporting resources					
AS-5.2. Take steps to prevent and minimize potential damage and interruption					
AS-5.3. Develop and document a comprehensive contingency plan					
AS-5.4. Periodically test the contingency plan and adjust it as appropriate					
Overall assessment of contingency planning					

Exposure Draft

Business Process Controls

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
BP-1 Transaction data input is complete, accurate, valid, and confidential					
BD-1.1. Transaction data strategy is properly defined, documented, and appropriate					
BP-1.2. Source documentation and input file data collection and input preparation and entry is effectively controlled					
BP-1.3. Access to data input is adequately controlled					
BP-1.4. Input data are approved					
BP-1.5. Input data are validated and edited to provide reasonable assurance that erroneous data are detected before processing					
BP-1.6. Input values to data fields that do not fall within the tolerances or parameters determined by the management result in an input warning or error					
BP-1.7. Error handling procedures during data origination and entry reasonably assure that errors and irregularities are detected, reported, and corrected					
BP-1.8. Errors are investigated and resubmitted for processing promptly and accurately					
Overall assessment of transaction data input controls					
BP-2. Transaction data processing is complete, accurate, valid, and confidential					
BP-2.1. Application functionality is designed to process input data, with minimal manual intervention					
BP-2.2. Processing errors are identified, logged and resolved					
BP-2.3 Transactions are executed in accordance with predetermined parameters and tolerances, specific to entity's risk management					
BP-2.4. Transactions are valid and unique (not duplicated)					
BP-2.5 The transactions are appropriately authorized					
BP-2.6. Data from subsidiary ledgers are in balance with the general ledger					
BP-2.7. User-defined processing is adequately controlled					
BP-2.8. As appropriate, the confidentiality of transaction data during processing is adequately controlled					
BP-2.9. An adequate audit and monitoring capability is implemented					
Overall assessment of transaction data processing controls					
BP-3. Transaction data output is complete, accurate, valid, and confidential					
BP-3.1. Outputs are appropriately defined by the management (output form, sensitivity of data, user selectivity, confidentiality, etc.)					

Exposure Draft

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
BP-3.2. Output generation and distribution are aligned with the reporting strategy					
BP-3.3. System generated outputs/reports are reviewed to reasonable assure the integrity of production data and transaction processing					
BP-3.4. Output//reports are in compliance with applicable laws and regulations					
BP-3.5. Access to output/reports and output files is based on business need and is limited to authorized users					
Overall assessment of data output controls					
BP-4. Master data setup and maintenance is adequately controlled					
BP-4.1. Master data are appropriately designed					
BP-4.2. Changes to master data configuration are appropriately controlled					
BP-4.3. Only valid master records exist					
BP-4.4. Master data are complete and valid					
BP-4.5. Master data are consistent among modules					
BP-4.6. Master data additions, deletions, and changes are properly managed and monitored by data owners					
BP-4.7. As appropriate, the confidentiality of master data is adequately controlled					
Overall assessment of master data setup and maintenance					

Interface Controls

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
IN-1. Implement an effective interface strategy and design					
IN-1.1. An interface strategy is developed for each interface used in the application					
IN-1.2. An interface design is developed for each interface used in the application that includes appropriate detailed specifications					
Overall assessment of interface strategy and design					
IN-2. Implement effective interface processing procedures					

Exposure Draft

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
IN-2.1. Procedures are in place to reasonably assure that the interfaces are processed accurately, completely, and timely					
IN-2.2. Ownership for interface processing is appropriately assigned					
IN-2.3. The interfaced data is reconciled between the source and target application to ensure that the data transfer is complete and accurate					
IN-2.4. Errors during interface processing are identified by balancing processing and promptly investigated, corrected, and resubmitted for processing					
IN-2.5. Rejected interface data is isolated, analyzed, and corrected in a timely manner					
IN-2.6. Data files are not processed more than once					
Overall assessment of interface controls					

Data Management System Controls

Critical elements	Are controls effective?			Comments on control effectiveness	Work paper references
	Yes	No	Partially		
DA-1. Implement an effective data management system strategy and design					
DA-1.1 Implement an effective data management system strategy and design, consistent with the control requirements of the application and data					

Exposure Draft

particular category. However, when the auditor considers control weaknesses identified in separate control categories collectively, it may justify concluding controls to be ineffective (cross-cutting). For example, the auditor may have identified weaknesses indicating that the entity did not have a complete inventory of all major systems (security management), the system configuration baseline was incomplete (configuration management), and all critical systems/activities for contingency planning may not have been identified. In assessing these weaknesses solely in the context of their respective control categories, the auditor may have concluded that they did not reach the threshold to assess each of these respective control categories as ineffective. However, when the auditor assessed the weaknesses collectively, the auditor may conclude controls to be ineffective since an incomplete inventory of systems could significantly hamper the entity's ability to ensure that current and complete security settings are installed on all systems and that contingency plans address each system in the event of operational disruptions.

The space above is provided to document those assessments that are not control category specific but are made from a collectively assessment of weaknesses identified in separate control categories.

Exposure Draft

Appendix IV - Mapping of FISCAM to SP 800-53

In table below, FISCAM is mapped to NIST Special Publication (SP) 800-53. To assist auditors, the individual FISCAM general and business process control activities are referenced to related NIST 800-53 controls.

FISCAM Controls

General Controls

Security Management:

- SM-1. Establish a security management program

- SM-2. Periodically assess and validate risks

- SM-3. Document security control policies and procedures

- SM-4. Implement effective security awareness and other security-related personnel policies

Related NIST 800-53 Controls

- PL-2 System Security Plan
- PL-3 System Security Plan Update
- PL-6 Security-Related Activity Planning
- SA-2 Allocation of Resources

- CA-4 Security Certification
- CA-6 Security Accreditation
- RA-2 Security Categorization
- RA-3 Risk Assessment
- RA-4 Risk Assessment Update

- See first control for each family (e.g., AC-1, AT-1)

- AT-2 Security Awareness
- AT-3 Security Training
- AT-4 Security Training Records
- PL-4 Rules of Behavior

Exposure Draft

FISCAM Controls

General Controls:

Security Management (cont'd):

SM-4 Implement effective security awareness and other security-related personnel policies (continued)

SM-5. Monitor effectiveness of the security program

SM-6. Effectively remediate information security weaknesses

SM-7. Ensure that activities performed by external parties third parties are adequately secure

Access Controls:

AC-1 Adequately protect information system boundaries

Related NIST 800-53 Controls

PS-1 Personnel Security Policy and Procedures

PS-2 Position Categorization

PS-3 Personnel Screening

PS-4 Personnel Termination

PS-5 Personnel Transfer

PS-6 Access Agreements

PS-7 Third-Party Personnel Security

PS-8 Personnel Sanctions

CA-2 Security Assessments

CA-7 Continuous Monitoring

PL-5 Privacy Impact Assessment

RA-5 Vulnerability Assessment

CA-5 Plan of Action and Milestones

AC-20 Use of External Information Systems

MA-4 Remote Maintenance

PS-7 Third-Party Personnel Security

SA-9 External Information System Services

AC-4 Information Flow Enforcement

Exposure Draft

FISCAM Controls

General Controls:

Access Controls:

AC-1 Adequately protect information system boundaries (continued)

AC-2. Implement effective identification and authentication mechanisms

Related NIST 800-53 Controls

AC-8 System Use Notification
AC-9 Previous Logon Notification
AC-11 Session Lock
AC-12 Session Termination
AC-17 Remote Access
AC-18 Wireless Access Restrictions
AC-19 Access Control for Portable and Mobile Devices
CA-3 Information System Connections
SC-7 Boundary Protection
SC-10 Network Disconnect

AC-7 Unsuccessful login attempts

AC-10 Concurrent Session Control
AC-14 Permitted Actions Without Identification and Authentication
AU-10 Non-Repudiation
IA-2 User Identification and Authentication
IA-3 Device Identification and Authentication
IA-4 Identified Management
IA-5 Authentication Management
IA-6 Authentication Feedback
SC-17 Public Key Infrastructure Certificates

Exposure Draft

FISCAM Controls

General Controls:

Access Controls:

AC-2. Implement effective identification and authentication mechanisms (continued)

AC-3. Implement effective authorization controls

AC-4. Adequately protect sensitive system resources

Related NIST 800-53 Controls

SC-20 Secure Name/Address Resolution Service (Authoritative Source)
SC-21 Secure Name Address Resolution Service
SC-22 Architecture and Provisioning for Name/Address Resolution Service
SC-23 Session Authenticity

AC-2 Account Management
AC-3 Access Enforcement
AC-6 Least Privilege
CM-7 Least Functionality
SC-6 Resource Priority
SC-14 Public Access Protections
SC-15 Collaborative Computing

AC-15 Automated Markings
AC-16 Automated Labeling
IA-7 Cryptographic Module Authentication
MP-2 Media Access
MP-3 Media Labeling
MP-4 Media Storage
MP-5 Media Transport
MP-6 Media Sanitation and Disposal
PE-19 Information Leakage
SC-2 Application Partitioning
SC-3 Security Function Isolation

Exposure Draft

FISCAM Controls

General Controls:

Access Controls:

AC-4. Adequately protect sensitive system Resources (continued)

AC-5. Implement an effective audit and monitoring capability

Related NIST 800-53 Controls

SC-4 Information Remnance
SC-8 Transmission Integrity
SC-9 Transmission Confidentiality
SC-11 Trusted Path
SC-12 Cryptographic Key Establishment and Management
SC-13 Use of Cryptography
SC-16 Transmission of Security Parameters
SC-18 Mobile Code

AC-13 Supervision and Review – Access Control

AT-5 Contacts with Security Groups and Associations

AU-2 Auditable Events
AU-3 Content of Audit Records
AU-4 Audit Storage Capacity
AU-5 Response to Audit Processing Failures
AU-6 Audit Reduction and Report Generation
AU-7 Audit Reduction and Report Generation
AU-8 Time Stamps
AU-9 Protection of Audit Information
AU-11 Audit Record Retention

IR- 1 Incident Response Policy
IR-2 Incident Response Training
IR-3 Incident Response Testing
IR-4 Incident Handling
IR-5 Incident Monitoring
IR-6 Incident Reporting
IR-7 Incident Response Assistance

Exposure Draft

FISCAM Controls

General Controls:

Access Controls:

AC-5. Implement an effective audit and monitoring capability (continued)

AC-6 Establish adequate physical security controls

Configuration Management:

CM-1. Develop and document CM policies, plans, and procedures

CM-2. Maintain current configuration identification information

CM-3. Properly authorize, test, approve, track and control all configuration changes

Related NIST 800-53 Controls

SC-5 Denial of Service Protection

SI-4 Information System Monitoring Tools and Techniques

SI-6 Security Functionality Verification

PE-2 Physical Access Authorization

PE-3 Physical Access Control

PE-4 Access Control for Transmission Medium

PE-5 Access Control Policy for Display Medium

PE-6 Monitoring Physical Access

PE-7 Visitor Control

PE-8 Access Records

CM-1 Configuration Management Policy and Procedures

CM-2 Baseline Configuration

CM-6 Configuration Settings

CM-8 Information System Component Inventory

SA-5 Information System Documentation

CM-3 Configuration Change Control

SA-2 Allocation Resources

SA-3 Life Cycle Support

SA-4 Acquisitions

SA-8 Security Engineering Principles

Exposure Draft

FISCAM Controls

General Controls:

Configuration Management:

CM-3. Properly authorize, test, approve, and track all configuration changes (continued)

CM-4. Routinely monitor the configuration

CM-5. Update software on a timely basis to protect against known vulnerabilities

CM-6 Appropriately document and approve emergency changes to the configuration

Related NIST 800-53 Controls

SA-10 Developer Configuration management

SA-11 Developer Security Testing

CM-4 Monitoring configuration Changes

CM-5 Access Restrictions for Change

SI-7 Software and Information Integrity

RA-5 Vulnerability Scanning

SA-6 Software Usage Restrictions

SA-7 User Installed Software

SC-19 Voice Over Internet Protocol

SI-2 Flaw Remediation

SI-3 Malicious Code Protection

SI-5 Security Alerts and Advisories

SI-8 Spam Protection

Exposure Draft

FISCAM Controls

General Controls:

Segregation of Duties:

- SD-1 Segregate incompatible duties and establish related policies
- SD-2 Control personnel activities through formal operating procedures, supervision, and review

Contingency Planning:

- CP-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources
- CP-2. Take steps to prevent and minimize potential damage and interruption

Related NIST 800-53 Controls

- AC-5 Separation of Duties
PS-2 Position Categorization
PS-6 Access Agreements
- AC-5 Separation of Duties
PS-2 Position Categorization
PS-6 Access Agreements
- CP-3 Contingency Training
CP-6 Alternate Storage Site
CP-7 Alternate Processing Site
CP-9 Information System Backup
CP-10 Information System Recovery and Backup
MA-2 Controlled Maintenance
MA-3 Maintenance Tools
MA-5 Maintenance Personnel
MA-6 Timely Maintenance
PE-9 Power Equipment and Power Cabling

Exposure Draft

FISCAM Controls

General Controls:

Continuity Planning:

CP-2. Take steps to prevent and minimize potential damage and interruption (continued)

CP-3. Develop and document a comprehensive contingency plan

CP-4. Periodically test the contingency plan and adjust it as appropriate

Related NIST 800-53 Controls

PE-10 Emergency Shutoff
PE-11 Emergency Power
PE-12 Emergency Lighting
PE-13 Fire Protection
PE-14 Temperature and Humidity Controls

PE-15 Water Damage Protection
PE-16 Delivery and Removal
PE-17 Alternate Work Site
PE-18 Location of Information System Documentation
SA-5 Information System Documentation

CP-2 Contingency Plan
CP-5 Contingency Plan Update
CP-8 Telecommunications services

CP-4 Contingency Plan Testing and Exercise
CP-5 Contingency Plan Update

Exposure Draft

FISCAM Controls

Business Process Application Level Controls:

Application Level General Controls:

- AS-1. Implement effective application security management
- AS-2. Implement effective application access controls
- AS-3. Implement effective application configuration management
- AS-4. Segregate application user access to conflicting transactions and activities and monitor segregation
- AS-5. Implement effective application contingency planning

Business Process Controls:

- BP-1. Transaction data input is complete, accurate, valid, and confidential

- BP-2. Transaction data processing is complete, accurate, valid, and confidential

Related NIST 800-53 Controls

The related NIST SP 800-53 application level general controls are identified under related General Controls above.

- SI-9 Information Input Restrictions
- SI-10 Information Accuracy, Completeness, Validity, and Authenticity
- SI-11 Error Handling

- SI-9 Information Input Restrictions
- SI-10 Information Accuracy, Completeness, Validity, and Authenticity
- SI-11 Error Handling

Exposure Draft

FISCAM Controls

Business Process Application Level Controls:

Business Process Controls:

BP-3. Transaction data output is complete, accurate, valid, and confidential

BP-4. Master data setup and maintenance is adequately controlled

Interface controls:

IN-1 Implement an effective interface strategy and design

IN-2 Implement effective interface processing procedures

Related NIST 800-53 Controls

SI-9 Information Input Restrictions
SI-10 Information Accuracy, Completeness, Validity, and Authenticity

SI-11 Error Handling

SI-12 Information Output Handling and Retention

SI-9 Information Input Restrictions

SI-10 Information Accuracy, Completeness, Validity, and Authenticity

SI-11 Error Handling

SI-9 Information input Restrictions

SI-10 Information Accuracy, Completeness, Validity, and Authenticity

SI-11 Error Handling

SI-9 Information input Restrictions

SI-10 Information Accuracy, Completeness, Validity, and Authenticity

SI-11 Error Handling

Exposure Draft

FISCAM Controls

Data management controls:

DA-1. Implement an effective data management system strategy and design

Related NIST 800-53 Controls

Exposure Draft

Appendix V - Knowledge, Skills, and Abilities Needed to Perform Information System Controls Audits

Information system (IS) controls audits require a broad range of technical skills. A key component of planning is determining the knowledge, skills, and abilities needed to perform the IS audit. Such needs are then compared with the audit team's current knowledge, skills, and abilities to identify any expertise that must be acquired. Any expertise gap can be filled through hiring, training, contracting, or staff sharing. The knowledge, skills, and abilities described in this appendix are not intended to be prescriptive, but to provide a framework to assist the auditor in determining the audit resources needed to effectively perform audit procedures in an IS audit. In addition, when contracting for IS audit services, this framework may be used as resource to identify the specific knowledge, skills, and abilities that will be needed to perform the contracting services requested.

Generally accepted government auditing standards (GAGAS) state that the "staff assigned to conduct an audit or attestation engagement under GAGAS must collectively possess the technical knowledge, skills, and experience necessary to be competent for the type of work being performed before beginning work on that assignment." The standards further require that if the work involves a review of information systems, the staff assigned to the GAGAS audit engagement should collectively possess knowledge of information technology.

⁹⁷These skills are often described in terms of knowledge, skills, and abilities (KSAs). KSAs are typically used in job position descriptions

⁹⁷ *Government Auditing Standards: July 2007 Revision (GAO-07-731G)*, paragraph 3.43.

Exposure Draft

and job announcements to describe the attributes required for those in particular jobs. These terms are defined as follows:

Knowledge—the foundation upon which skills and abilities are built. Knowledge is an organized body of information, facts, principles, or procedures that, if applied, make adequate performance of a job possible. An example is knowledge of tools and techniques used to establish logical access control over an information system.

Skill—the proficient manual, verbal, or mental manipulation of people, ideas, or things. A skill is demonstrable and implies a degree of proficiency. For example, a person may be skilled in operating a personal computer to prepare electronic spreadsheets or in using a software product to conduct an automated review of the integrity of an operating system.

Ability—the power to perform a job function while applying or using the essential knowledge. Abilities are evidenced through activities or behaviors required to do a job. An example is the ability to apply knowledge about logical access controls to evaluate the adequacy of an organization's implementation of such controls.

A staff member's knowledge, skills, and abilities can be categorized in accordance with FISCAM audit areas. Table 1 includes an overview of the knowledge, skills, and abilities that a team typically needs to effectively perform an IS audit. It assumes a level of proficiency in performing basic auditing tasks, such as interviewing, gathering and documenting evidence, communicating both orally and in writing, and managing projects. It focuses on attributes associated specifically with IS auditing. Although each staff member assigned to such an audit need not have all these attributes, the audit team must collectively possess the KSA's necessary to perform the audit, including adequately planning the audit, assessing the effectiveness of IS controls, testing IS controls, determining the effect of the results of testing on the audit objectives, developing findings and recommendations, and reporting the results. Audit resources may be supplemented from outside the organization through partnering or engaging consultants.

Exposure Draft

Table 1. Knowledge, Skills, and Abilities for IS Security Audit Areas by FISCAM Objective

FISCAM objective	Associated knowledge, skills, and abilities
Security Management	<ul style="list-style-type: none">• Knowledge of the legislative requirements for an entity's information security management program• Knowledge of the sensitivity of data and the risk management process through risk assessment and risk mitigation• Knowledge of the risks associated with a deficient information security management program• Knowledge of the key elements of a good information security management program• Ability to analyze and evaluate an entity's security policies and procedures and identify their strengths and weaknesses• Ability to analyze and evaluate the entity's security management program and identify the strengths and weaknesses, including:<ul style="list-style-type: none">• security management program, structure, and responsibilities, including system inventories• risk assessment• security awareness training for employees, contractors, third parties (including those in sensitive security and data processing position) and security-related personnel policies (including personnel hiring, including reference and background checks, and job transfers and terminations),• performance of periodic tests and evaluations of IS controls and monitoring to ensure compliance with established policies and procedures (including copies of tests and evaluations performed), and• security requirements and monitoring activities of third-party providers supporting specific application(s).

Exposure Draft

FISCAM objective	Associated knowledge, skills, and abilities
Access Control	<ul style="list-style-type: none">• Knowledge across platforms of the access paths into computer systems and of the functions of associated hardware and software that provides an access path• Knowledge of access level privileges granted to users and the technology used to provide and control them• Knowledge of the procedures, tools, and techniques that provide for good physical, technical, and administrative controls over access• Knowledge of the risks associated with inadequate access controls• Skills to perform vulnerability assessments of the entity's applications and supporting computer systems• Ability to analyze and evaluate the entity's access controls and identify the strengths and weaknesses, including:<ul style="list-style-type: none">• system boundaries• controlling remote access to agency information, including use of remote devices,• user and system identification and authentication,• requesting, approving, and periodically reviewing user access authorization,• restricting access to sensitive system resources (including system utilities, system software, and privileged accounts),• protecting digital and sensitive media, including portable media,• applying cryptography methods, if used,• monitoring mainframe, mid-level servers, and network systems for incidents, including management response and reporting on unusual activities, intrusion attempts, and actual intrusions, and• controlling physical security, including granting and controlling of physical access to the data center and other IT sensitive areas.

Exposure Draft

FISCAM objective	Associated knowledge, skills, and abilities
Configuration Management	<ul style="list-style-type: none">• Knowledge of the concept of configuration management and the System Development Life Cycle (SDLC) process• Knowledge of baseline configuration management procedures, tools, and techniques that provide control over application and system software, and computer security settings• Knowledge of the risks associated with the modification, including emergency changes, of application and system software, and computer security settings• Knowledge of the risks associated with inadequate procedures for updating software to protect against known vulnerabilities• Ability to analyze and evaluate the entity's configuration management and identify the strengths and weaknesses, including:<ul style="list-style-type: none">• configuration management policies, including the approval and testing of scheduled and emergency changes, and monitoring procedures to ensure compliance,• maintaining current configuration information,• authorizing, testing, approving, and tracking all configuration changes,• monitoring/auditing the configuration,• patch management, vulnerability scanning, virus protection, emerging threats, and user installed software, and• emergency changes.
Segregation of Duties	<ul style="list-style-type: none">• Knowledge of the different functions involved with information systems and data processing and incompatible duties associated with these functions• Knowledge of the risks associated with inadequate segregation of duties• Ability to analyze and evaluate the entity's organizational structure and segregation of duties (including periodic review of access authorizations) and identify the strengths and weaknesses
Contingency Planning	<ul style="list-style-type: none">• Knowledge of the procedures, tools, and techniques that provide for contingency planning and business continuity• Knowledge of the risks that exist when measures are not taken to provide for contingency planning and business continuity• Ability to analyze and evaluate an entity's contingency planning program and contingency plans for business continuity and identify the strengths and weaknesses, including:<ul style="list-style-type: none">• assessing the availability needs of entity systems• backing-up data, programs, and software, and• environmental controls, including emergency power, fire/smoke detection and response, hardware maintenance and problem management, alternate work sites, etc.

Exposure Draft

FISCAM objective	Associated knowledge, skills, and abilities
Business Process Controls	<ul style="list-style-type: none"> • Knowledge about the practices, procedures, and techniques that provide for the completeness, accuracy, validity, and confidentiality of application data • Knowledge of typical applications in each business process transaction cycle • Skills to use a generalized audit software package to conduct data analyses and tests of application data, and to plan, extract, and evaluate data samples • Ability to analyze and evaluate the entity's application controls and identify the strengths and weaknesses

Source: GAO.

Auditors performing tasks in two of the above FISCAM areas—**Access Controls and Configuration Management**—require additional specialized technical skills. Such technical specialists should have skills in one or more of the categories listed in table 2.

Table 2. KSAs for Information Security Technical Specialists

Specialist	Skills
Network analyst	<ul style="list-style-type: none"> • Advanced knowledge of network hardware and software • Understanding of data communication protocols • Ability to evaluate the configuration of routers, firewalls, and intrusion detection systems • Ability to perform external and internal vulnerability tests with manual and automated tools • Knowledge of the operating systems used by servers
Windows/Novell analyst	<ul style="list-style-type: none"> • Detailed understanding of microcomputer and network architectures • Ability to evaluate the configuration of servers and the major applications hosted on servers • Ability to perform internal vulnerability tests with manual and automated tools
Unix analyst	<ul style="list-style-type: none"> • Detailed understanding of the primary variants of the Unix architectures • Ability to evaluate the configuration of servers and the major applications hosted on servers • Ability to perform internal vulnerability tests with manual and automated tools
Database analyst	<ul style="list-style-type: none"> • Understanding of the control functions of the major database management systems • Understanding of the control considerations of the typical application designs that use database systems • Ability to evaluate the configuration of major database software products

Exposure Draft

Specialist	Skills
Mainframe system software analyst	<ul style="list-style-type: none">• Detailed understanding of the design and function of the major components of the operating system• Ability to develop or modify tools necessary to extract and analyze control information from mainframe computers• Ability to use audit software tools• Ability to analyze modifications to system software components
Mainframe access control analyst	<ul style="list-style-type: none">• Detailed understanding of auditing access control security software such as ACF2, Top Secret, and RACF• Ability to analyze mainframe audit log data• Ability to develop or modify tools to extract and analyze access control information

Source: GAO.

As table 2 shows, some activities require a high degree of IT knowledge, skills, and abilities, while others involve more basic auditing tasks (interviewing, gathering background information, and documenting the IT security environment). Audit management may therefore want to organize staff that have highly specialized technical skills into a separate group that has access to special-purpose computer hardware and software. A group of this kind can focus on more technical issues, while other groups within the organization can perform the less technical work.

Exposure Draft

Appendix VI - Scope of an Information System Controls Audit in Support of a Financial Audit

This appendix provides a framework for assessing the effectiveness of information system controls audits in support of financial statement audits. Given the prevalence of the use of information systems to process financial information, performing a financial audit generally includes an assessment of the effectiveness of information system controls. The information system controls audit should be performed as an integral part of the financial audit.

This appendix is intended to assist (1) financial auditors in communicating audit requirements to IS control specialists, and (2) financial auditors and IS control specialists in understanding how an assessment of the effectiveness of IS controls integrates with financial audit requirements.

The Government Accountability Office (GAO) and the President's Council on Integrity and Efficiency (PCIE) *Financial Audit Manual* (FAM) presents a methodology for performing financial statement audits of federal entities in accordance with professional standards. Chapter 2 (and related steps in Chapter 4) of the FISCAM describe a methodology for performing the IS controls audit in the context of an audit performed in accordance with generally accepted government auditing standards (GAGAS). This appendix discusses how the audit steps described in Chapter 2 of the FISCAM (and related steps in Chapter 4) provide more specific guidance concerning the evaluation of the effectiveness of information systems controls in support of the audit steps in the FAM. For financial audits performed in accordance with the FAM, the steps in the FISCAM should be performed in coordination with the related steps in the FAM. The flowchart of steps in assessing IS controls in a

Exposure Draft

financial statement audit, appearing in FAM 295 J, is presented at the end of this appendix.

The following table presents a summary of the relationship between selected FAM steps and related FISCAM steps.

FAM Step(s)	Related FISCAM Step(s)
AUDIT PLANNING	
220 Understand the Entity's Operations 235 Identify Significant Line Items, Accounts, Assertions, and RSSI 240 Identify Significant Cycles, Accounting Applications, And Financial Management Systems	2.1.1 Planning the Information System Controls Audit— Overview 2.1.2 Understand the Overall Audit Objectives and Related Scope of the Information System Controls Audit 2.1.3 Understand the Entity's Operations and Key Business Processes 2.1.4 Obtain a General Understanding of the Structure of the Entity's Networks 2.1.5 Identify Key Areas of Audit Interest (files, applications, systems, locations)
260 Identify Risk Factors	2.1.6 Assess Information system Risk on a Preliminary Basis
270 Determine Likelihood of Effective IT System Controls	2.1.7 Identify Critical Control Points (for example, external access points to networks) 2.1.8 Obtain a Preliminary Understanding of Information System Controls

Exposure Draft

Miscellaneous FAM planning sections	2.1.9 Perform Other Audit Planning Procedures
INTERNAL CONTROL TESTING	
310 Overview of the Internal Control Phase 320 Understand Information Systems 330 Identify Control Objectives 340 Identify and Understand Relevant Control Activities 350 Determine the Nature, Timing, and Extent of Control Tests And Of Tests For Systems' Compliance With FFMIA Requirements 360 Perform Nonsampling Control Tests And Tests For Systems' Compliance With FFMIA Requirements, including 360.03-.09--Test IT System Controls	2.2 Perform Information System Controls Audit Tests <ul style="list-style-type: none"> • Understand Information Systems Relevant to the Audit Objectives • Identify IS Control Techniques Relevant to the Audit Objectives • Test IT System Controls
REPORTING THE RESULTS OF THE IS CONTROLS AUDIT	
370 Assess Controls On A Preliminary Basis 580 Draft Reports – Internal Control	2.3 Report Audit Results

AUDIT PLANNING

IS Audit Resources

As discussed in FAM Section 110.27, the audit team should possess sufficient knowledge of IS controls to determine the effect of IT on the audit, to understand IS controls, and to consult with an IS

Exposure Draft

controls specialist⁹⁸ to design and test IS controls. Specialized IS audit skills generally are needed in situations where

- the entity's systems, automated controls, or the manner in which they are used in conducting the entity's business are complex;
- significant changes have been made to existing systems or new systems have been implemented;
- data are extensively shared among systems;
- the entity participates in electronic commerce;
- the entity uses emerging technologies; or
- significant audit evidence is available only in electronic form.

In some cases, the financial auditor may consult with IS controls specialists within the audit organization or use outside contractors to provide these skills. However, per AU 311.22, the financial auditor should have sufficient knowledge to communicate the objectives of the specialists' work, to evaluate whether the specified procedures will meet the audit objectives, and to evaluate the results of the procedures as they relate to the nature, extent, and timing of further planned audit procedures.

Appendix V of the FISCAM provides a framework to assist the auditor in determining the audit resources needed to effectively perform an IS controls audit. In addition, when contracting for IS systems audit services, this framework may be used as a resource to identify the specific knowledge, skills, and abilities that will be needed to perform the contracting services requested. Section 2.1.9.C "Audit Resources" in Chapter 2 provides additional information on the use of IS controls specialists in a GAGAS audit.

⁹⁸ The IS control specialist is a person with technical expertise in information technology systems, general controls, business process applications and controls, and information security.

Exposure Draft

The following sections discuss IT-related FAM steps and the related FISCAM steps.

Understand the Entity's Operations, Identify Significant Line Items, Accounts, Assertions, and RSSI, and Identify Significant Cycles, Accounting Applications, and Financial Management Systems

FAM 220.01 states that the auditor must obtain an understanding of the entity and its environment, including internal control to assess the risk of material misstatement of the financial statements, whether due to error or fraud, and to design the nature, extent, and timing of further audit procedures. The following IT-related FAM sections discuss obtaining an understanding of the entity's operations and information systems:

- 220.04—the auditor should identify significant external and internal factors that affect the entity's operations as part of understanding the entity and its environment for purposes of planning the audit, including the IT structure and the extent to which IT processing is performed externally such as through cross-servicing agreements.
- 220.07—the auditor should develop and document a high-level understanding of the entity's use of IS controls and how IT affects the generation of financial statement information and supplementary information. An IS controls specialist may assist the auditor in understanding the entity's use of IS controls. Appendix I of the FISCAM may be used to document this understanding.
- 235.01—the auditor should identify significant line items and accounts in the financial statements and significant related financial statement assertions.
- 240.08—once the auditor identifies significant accounting applications, the auditor should determine which information systems are involved in those applications.
- 240.09—the auditor should obtain sufficient knowledge of the information systems relevant to financial reporting to

Exposure Draft

understand the accounting processing from initiation of a transaction to its inclusion in the financial statements, including electronic means used to transmit, process, maintain, and access information (see AU 319.49, SAS No. 94).

The following FISCAM sections (Chapter 2) provide more specific guidance on how the auditor obtains an understanding of the entity's IT operations and information systems:

- Planning the information system controls audit—overview – 2.1.1
- Understand the entity's operations and key business processes - 2.1.3
- Obtain a general understanding of the structure of the entity's networks – 2.1.4
- Identify key areas of audit interest (files, applications, systems, locations) – 2.1.5

More specifically, based on the audit objectives and the auditor's understanding of the business processes and networks, the auditor's identification of key areas of audit interest includes:

- key business process applications and where each key business process application is processed,
- key data files used by each key business application, and
- relevant general controls at the entitywide and system levels, upon which application level controls depend.

These FISCAM sections include information related to the IS controls audit that should be included in audit documentation. Such information should be summarized, as appropriate, in the entity profile or an equivalent document, as discussed in FAM Section 290.04. However, the auditor generally should document internal control separately as discussed below and in FAM 390.

Identify Risk Factors

FAM Section 260.09 states that the auditor should (1) identify conditions that significantly increase inherent, fraud, and control risk (based on identified control environment, risk assessment, communication, or monitoring weaknesses) and (2) conclude

Exposure Draft

whether any identified control risks preclude the effectiveness of specific control activities in significant applications. The auditor should identify specific inherent risks, fraud risks, and control environment, risk assessment, communication, and monitoring weaknesses based on information obtained in the planning phase, primarily from understanding the entity's operations, including significant IT processing performed outside the entity and preliminary analytical procedures. SAS No. 70 reports, which are discussed further in FAM 310 and in Appendix VII, may be prepared by service auditors for organizations performing significant IT processing for the entity. The auditor may find these reports useful for performing risk assessments and planning other audit procedures. The auditor should update the risk assessment throughout the audit.

FAM Section 260.22 states that IS controls do not affect the audit objectives for an account or a cycle. However, IS controls can introduce inherent risk factors not present in a manual accounting system. The FAM section states that the auditor should assess the overall impact of IS processing on inherent risk. The impact of these factors typically will be pervasive in nature. An IS controls specialist may assist the auditor in considering these factors and making this assessment.

FAM Section 260.56 states that IS controls affect the effectiveness of control activities, the control environment, risk assessment, communication, and monitoring. For example, controls that normally would be performed by separate individuals in manual systems may be concentrated in one computer application and pose a potential segregation-of-duties issue. See SAS No. 109.57-63 for further discussion of the effect of IT on internal control.

FAM Section 260.57 provides several IS factors, discussed in Chapter 2 of the FISCAM, that the auditor should evaluate in making an overall assessment of the control environment, risk assessment, communication, and monitoring.

The FISCAM section 2.1.6 entitled "Assess Information System Risk on a Preliminary Basis" provides more specific guidance on how the auditor identifies IS risk (inherent and the control environment, risk assessment, communication, and monitoring components of internal

Exposure Draft

control). Also, the FISCAM section 2.1.9.B entitled “Consideration of the Risk of Fraud” provides more specific guidance concerning identification of the risk of fraud arising from IT, including coordination between the financial auditor and the IS controls specialist. In addition, the FISCAM section 2.5.1 “Additional IS Risk Factors” provides more risk factors for the auditor to consider. Further, FISCAM Appendix VII provides more information on the use of SAS 70 reports.

These FISCAM sections include information that should be included in audit documentation. In addition, such information should be summarized, as appropriate, in the GRA or equivalent document as discussed in FAM Section 290, including:

- the assessments of overall inherent risk and the risk factors considered in the assessment, and
- the assessments of the overall effectiveness of the control environment, risk assessment, communication, and monitoring, including whether an ineffective control environment precludes the effectiveness of specific control activities.

Determine Likelihood of Effective IS Controls

As discussed in FAM 270, information system (IS) controls consist of those internal controls that are dependent on information systems processing and include general, business process application, and user controls. IS controls consist of those internal controls that are dependent on information systems processing and include general controls (entitywide, system, and business process application levels), business process application controls (input, processing, output, master file, interface, and data management system controls), and user controls (controls performed by people interacting with information systems). General and business process application controls are always IS controls. A user control is an IS control if its effectiveness depends on information systems processing or the reliability (accuracy, completeness, and validity) of information processed by information systems. Conversely, a user control is not an IS control if its effectiveness does not depend on information systems processing or the reliability of information processed by information systems.

Exposure Draft

In the financial audit planning phase, the auditor, with the assistance of an IS control specialist should determine whether IS controls are likely to be effective and should therefore be considered in the internal control phase. The auditor may coordinate work done to meet the provisions of FISMA with work done as part of the financial statement audit.

The procedures performed to determine the likelihood of effective IS controls build on those procedures performed while understanding the entity's operations and assessing the effects of IS controls on inherent risk and the control environment, risk assessment, communication, and monitoring. Under SAS No. 109, the auditor should sufficiently understand each of the five components of internal control—control environment, risk assessment, information and communication, monitoring, and control activities—to assess the risk of material misstatement. This understanding should include relevant IS aspects.

As discussed in FAM 260.06, the auditor evaluates and tests the following types of controls in a financial statement audit:

- financial reporting controls,
- compliance controls, and
- certain operations controls (to the extent described in FAM 275).

For each of the specific controls to be evaluated and tested, as documented in the SCE Form or equivalent, the auditor should distinguish which are IS controls. In addition, based on such IS controls and the audit planning procedures (particularly the identification of critical control points), the auditor should identify those other IS controls (general and business process application controls) upon which the effectiveness of the controls in the SCE depend. These other IS controls also need to be effective for the specific controls in the SCE to be effective. FISCAM Appendices II and III can be used to document such controls.

IS controls can be classified into three types:

- general controls – GAGAS defines information systems general controls as the policies and procedures that apply to all or a large segment of an entity's information systems. General controls help ensure the proper operation of information

Exposure Draft

systems by creating the environment for proper operation of application controls. General controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning.

- business process application controls –GAGAS defines application controls, sometimes referred to as business process controls, as those controls that are incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of transactions and data during application processing. Application controls include controls over input, processing, output, master data, application interfaces, and data management system interfaces.
- user controls – portions of controls that are performed by people interacting with IS controls. The effectiveness of user controls typically depend on the accuracy of the information produced by the IS controls.

An IS controls specialist generally should review and concur with the auditor’s identification of IS controls.

Testing of technical IS controls should be performed by an IS controls specialist as described in FAM 360. The audit team may work with the IS controls specialist by testing user controls and application controls involving manual follow-up.

FAM Section 270.05 states that early in the audit’s planning phase, the auditor and the IS controls specialist should understand the design of each of the three types of IS controls (general, business process application level, and user controls) to the extent necessary to tentatively conclude whether these controls are likely to be effective.

If they are likely to be effective, the auditor should consider specific IS controls in determining whether control objectives are achieved in the internal control phase. As discussed in SAS No. 109.54, evaluating the design of a control involves considering whether the control, individually or in combination with other controls, is capable of effectively preventing, detecting, and correcting material misstatements.

Exposure Draft

If IS controls are not likely to be effective, the auditor, with the assistance of the IS controls specialist, should obtain a sufficient understanding of control risks arising from IS controls to

- identify types of potential misstatements,
- consider factors that affect the risks of material misstatement,
- design tests of controls and substantive procedures, and
- develop appropriate findings.

Also, in the internal control phase, the auditor generally should focus on the effectiveness of manual controls in achieving control objectives, including manual controls that may mitigate weaknesses in IS controls. If IS controls are not likely to be effective due to poor general controls and if manual controls do not achieve the control objectives, the auditor should identify and evaluate any specific IS controls that are designed to achieve the control objectives to develop recommendations for improving internal controls.

As discussed in SAS No. 109.117-120, in some circumstances, such as where a significant amount of information is electronically initiated, recorded, processed, and reported, it may not be practical or possible to restrict detection risk to an acceptable level by performing only substantive tests for one or more financial statement assertions. In such circumstances, the auditor should test IS controls to obtain evidential matter about the effectiveness of both the design and operation of controls to reduce the assessed level of the risk of material misstatement.

The following FISCAM sections provide more specific guidance on how the auditor determines the likelihood of effective IS controls:

- Identify critical control points (for example, external access points to networks) – 2.1.7
- Obtain a preliminary understanding of information system controls – 2.1.8

These FISCAM sections include information that should be included in audit documentation. In addition to this audit documentation, as discussed in FAM Section 290, the auditor should document tentative conclusions on the likelihood that IT controls and any compensating controls such as manual controls, reviews, or reconciliations are operating effectively.

Exposure Draft

Other Audit Planning Procedures

The FISCAM section 2.1.9 provides additional information concerning the following planning steps in the IS controls audit that should be coordinated with the financial audit.

- Relevant laws and regulations—this section provides more specific guidance on how the auditor identifies significant IT related provisions of laws and regulations and should be performed in coordination with FAM Section 245
- Consideration of the risk of fraud—as discussed above, this section provides more specific guidance on how the auditor identifies the risk of fraud arising from IT, including coordination between the financial auditor and the IS controls specialist, and should be performed in coordination with FAM Section 260.
- Audit Resources—as discussed above, this section provides more specific guidance on how the auditor identifies the knowledge, skills, and abilities needed to perform an IS controls audit and the auditor’s responsibilities and procedures for using the work of an IS controls specialist, and should be performed in coordination with FAM Section 110.
- Multiyear testing plans—this section provides more specific guidance on how the auditor establishes a multiyear testing plan for IS controls, and should be performed in coordination with FAM Section 395G.
- Communication with entity management and those charged with governance—this section provides more specific guidance on communicating relevant IT-related information with entity management and those charged with governance, and should be performed in coordination with FAM Section 215.
- Service organizations—this section provides more specific guidance on the auditor’s consideration of IS controls, significant to the IS audit, that are performed by a service organization. This issue is discussed further in Appendix VII “Entity’s Use of Service Organizations”. This section should be performed in coordination with FAM 310.
- Using the work of others—this section provides more specific guidance on how the auditor prepares uses the work of others in performing the IS controls audit, and should be performed in coordination with FAM section 650.

Exposure Draft

- Audit plan—this section provides more specific guidance on how the auditor prepares an audit plan and strategy for performing the IS controls audit, and should be performed in coordination with FAM section 290.

Also the FISCAM provides more specific guidance on how the auditor documents the planning of the IS controls audit, and should be performed in coordination with FAM Section 290.

INTERNAL CONTROL TESTING

Overview

In general, FAM Section 300 describes the methodology for assessing the effectiveness of internal control in a financial audit. FAM Section 310 summarizes the methodology. Specifically, Section 310 states that, in the internal control phase, the auditor should gain an understanding of internal control and obtain evidence about the effectiveness of internal control to (1) assess control risk, (2) determine the nature, timing, and extent of control, compliance, and substantive testing, and (3) form an opinion or report on internal control over financial reporting and compliance. Control risk should be assessed separately for each significant financial statement assertion in each significant cycle/accounting application (including RSSI).

The auditor of federal financial statements must evaluate and test certain controls. AU 319 permits the auditor to assess control risk at a high (maximum) level and forgo evaluation and testing of financial reporting controls if the auditor believes evaluating their effectiveness would be inefficient. However, because OMB audit guidance requires the auditor to perform sufficient tests of internal controls that have been properly designed and placed in operation to support a low assessed level of control risk, the auditor in a federal financial audit may not elect to forgo control tests solely because it is more efficient to extend compliance and substantive audit procedures.

Exposure Draft

The following are the types of controls tested in a financial audit:

- financial reporting controls (including certain safeguarding and budget controls) for each significant assertion in each significant cycle/accounting application (identified in section 240),
- compliance controls for each significant provision of laws and regulations (identified in section 245), including budget controls for each relevant budget restriction (identified in section 250), and
- operations controls for each operations control (1) relied on in performing financial audit procedures or (2) selected for testing by the audit team. (see section 275).

The auditor is not required to test controls that have not been properly designed and implemented (placed in operation). Thus, internal controls that are not effective in design do not need to be tested. If the auditor determined in a prior year that controls in a particular accounting application were ineffective and if management indicates that controls have not improved, the auditor need not test them.

On the other hand, if controls have been determined to be effective in design and implemented (placed in operation), the auditor of federal financial statements must perform sufficient tests of their effectiveness to support a low assessed level of control risk. In such cases, the auditor may consider using a rotation approach to testing controls over the various accounting applications, as described in FAM Section 395 G (and in the FISCAM section 2.1.9.D “Multiyear Testing Plans”). If the auditor expects to disclaim an opinion because of scope limitations or inadequate controls, the auditor may limit internal control work to updating the understanding of controls and whether they have been placed in operation. The auditor may do this by inquiring as to whether previously identified control weaknesses have been corrected. In the year the auditor expects to issue an opinion on the financial statements, the auditor needs a basis of sufficient work on internal control.

Exposure Draft

In the internal control phase of a financial audit, the auditor should perform and document the following procedures:

- Understand the entity's information systems for financial reporting, compliance with laws and regulations, and relevant operations (see FAM Section 320).
- Identify control objectives (see FAM Section 330).
- Identify and understand relevant control activities that effectively achieve the control objectives (see FAM Section 340).
- Determine the nature, timing, and extent of control testing (see FAM Section 350).
- Perform control tests that do not involve sampling (nonsampling control tests - see section 360).1 (Sampling control tests, if necessary, are performed in the testing phase, as discussed in FAM Section 450.)
- On a preliminary basis, based on the evidence obtained, assess (1) the effectiveness of financial reporting, compliance, and relevant operations controls and (2) control and combined risk (see FAM Section 370). (Combined risk, which includes inherent and control risk, is discussed in FAM paragraph 370.09).

As discussed in FAM Section 310.10, in gaining an understanding of an entity's internal control, including internal control related to IT and other business processing performed outside the entity, the auditor should obtain evidence about the design of relevant controls and whether they have been placed in operation. In obtaining evidence about whether controls have been placed in operation, the auditor should determine whether the entity is using them, rather than merely having them written in a manual, for example. This differs from determining a control's operating effectiveness, which is concerned with how the control was applied, the consistency with which it was applied, and by whom. Gaining an understanding of the design of internal control does not require that the auditor obtain evidence about operating effectiveness.

As discussed in FAM Section 310.11, the auditor should obtain an understanding of internal control for IT and other business processing performed outside the entity under a service agreement or other contract arrangements for assessing risk and planning other audit procedures. The auditor may obtain this understanding by performing work directly at the service organization or by using SAS

Exposure Draft

No. 70 reports that include these internal controls as discussed in AU 324.06-.21.

For each potential weakness, consider the impact of compensating controls or other factors that mitigate or reduce the risks related to potential weaknesses.

The following sections summarize FAM audit steps related to the testing of information system controls. The auditor should coordinate these steps with the related FISCAM steps.

Understand Information Systems

FAM Section 320 states that the auditor may use an IS controls specialist to assist in understanding and documenting the IT aspects of these systems. The auditor should document the understanding of these systems in cycle memorandums, or other equivalent narratives, and generally should prepare or obtain related flow charts. FAM 340 and 350 discuss identifying and documenting controls that are designed to mitigate the risk of material misstatement.

Walk-throughs are important for understanding the transaction process and for determining appropriate audit procedures. The auditor should perform walk-throughs for all significant accounting applications. Walk-throughs of budget, accounting, compliance, and operations systems provide evidence about the functioning of such systems. The auditor should document these walk-throughs. The auditor should incorporate the IT aspects of each system into the audit documentation and may include additional flow charts, narratives, and checklists.

FAM Section 320 continues that the auditor should obtain an understanding of and should document the following for each significant cycle and accounting application (including those dealing with RSSI):

- The manner in which transactions are initiated;
- The nature and type of records, journals, ledgers, and source documents, and the accounts involved;

Exposure Draft

- The processing involved from the initiation of transactions to their inclusion in the financial statements, including the nature of computer files and the manner in which they are accessed, updated, and deleted; and
- The process used to prepare the entity's financial statements and budget information, including significant accounting estimates, disclosures, and computerized processing.

FAM Section 320.03 states that for each significant cycle and accounting application identified for significant line items and assertions in FAM 240 (including those dealing with RSSI) the auditor should obtain an understanding of and should document, among other things, processes used to prepare the entity's financial statements and budget information, including significant accounting estimates, disclosures, and IT processing. These processes include

- Procedures used to enter transaction totals into the general ledger;
- procedures used to initiate, authorize, record, and process journal entries in the general ledger;
- procedures used to record recurring and nonrecurring adjustments to the financial statements;
- procedures used to combine and consolidate general ledger data; and
- closing process, including manual and automated procedures, for preparing the financial statements and related disclosures.

The FISCAM section entitled "Understand Information Systems Relevant to the Audit Objectives" included in section 2.2 provides more specific guidance on how the auditor obtains an understanding of information systems. This FISCAM section includes information that should be included in audit documentation. As discussed in FAM Section 320, the auditor must document the understanding gained of each component of internal control, including the information system. The auditor should prepare sufficient documentation to clearly describe the accounting system. For each significant cycle, the auditor should prepare a cycle memorandum or equivalent. Also, the auditor generally should prepare an illustrative flowchart of the cycle and component accounting application(s). Flowcharts provide a good mechanism to document the process and the flow of transactions through the system.

Exposure Draft

However, the auditor should avoid extreme detail, which makes the charts confusing and hard to follow. Complex systems, particularly those involving IT, may be difficult to understand without a flowchart. To the extent required as described above, the auditor should use the following documents or equivalents to document.

Identify Relevant Control Objectives

FAM Section 330 discusses the identification of control objectives. In a financial audit, the auditor should identify control objectives for each type of control that if achieved, would provide the entity with reasonable assurance that individual and aggregate misstatements (whether caused by error or fraud), losses, or noncompliance material to the financial statements would be prevented or detected. For Required Supplementary Stewardship Information (RSSI), the Statement of Social Insurance, and nonmonetary information in the financial statements, such as physical units of heritage assets, the objectives would relate to controls that would provide reasonable assurance that misstatements, losses, or noncompliance that would be considered material by users of the information would be prevented or detected. As noted above, control objectives in a financial audit involve:

- financial reporting controls, including safeguarding controls and segregation-of-duties controls,
- compliance controls,
- budget controls, and
- relevant operations controls.

As discussed in FAM Section 495A.21, if the reliability of internally-generated data used in the substantive analytical procedures is dependent on the effectiveness of IS controls, the auditor should perform additional procedures before relying on the data. The auditor should test, as appropriate, (1) the relevant general controls and the specific business process application level controls over the data and/or (2) the data in the report.

The FISCAM section “Identify IS Control Techniques That are Relevant to the Audit Objectives” included in section 2.2 provides more specific guidance on how the auditor identifies relevant IS control activities. This FISCAM section includes information that

Exposure Draft

should be included in audit documentation. In addition to such documentation, as discussed in FAM Sections 390 and 395H, the auditor documents relevant control objectives in the SCE form or equivalent documentation. Based on such controls and the audit planning procedures (particularly the identification of critical control points), the auditor should identify those other IS controls (general, business process application, interface, and data management system controls) upon which the controls in the SCE depend. FISCAM Appendices II and III can be used to document such controls.

Identify Relevant Control Activities

As discussed in FAM Section 340, the auditor identifies and understands relevant control activities. For each control objective, based on discussions with entity personnel and the results of other procedures performed, the auditor should identify the control activities designed to achieve the specific control objective. The auditor may indicate these controls in the auditor's informal notes and/or interview write-ups for use in the following procedures, but the auditor need not formally document them on the SCE worksheet at this time. The auditor should first screen the activities to identify those that are effective and efficient to test. An IS controls specialist may assist the auditor in identifying and understanding IT controls. As discussed in FAM 350, the auditor should use walk-throughs to confirm that the entity has implemented these controls identified for further audit procedures. These walk-throughs are in addition to those performed earlier to understand the transaction processing. As discussed in FAM 270, in determining whether control objectives are achieved, the auditor should consider both manual and IS controls, if likely to be effective.

FAM Section 340.05 states that the auditor also should evaluate the appropriateness of the specified criteria used to identify items in a management or exception report. For example, IT input controls (such as the matching of vendor invoices with receiving reports and purchase orders) that require exact matches of data from different sources before a transaction is accepted for processing may be more effective than controls that accept transactions that fall within a broader range of values. On the other hand, controls based on exception reports that are limited to selected information or use

Exposure Draft

more selective criteria may be more effective than lengthy reports that contain excessive information.

The FISCAM section “Identify IS Control Techniques That are Relevant to the Audit Objectives” provides more specific guidance on how the auditor identifies relevant IS controls.

The FISCAM is organized in a hierarchical structure to assist the auditor in performing the IS controls audit. Chapter 3 (general controls) and Chapter 4 (business process application level controls) contain several control categories, which are groupings of related controls pertaining to similar types of risk. For each control category, the manual identifies critical elements—tasks that are essential for establishing adequate controls within the category. For each critical element, there is a discussion of the associated objectives, risks, and control activities, as well as related potential control techniques and suggested audit procedures. This hierarchical structure facilitates the auditor’s audit planning and the auditor’s analysis of identified control weaknesses.

Because control activities are generally necessary to achieve the critical elements, they are generally relevant to a GAGAS audit unless the related control category is not relevant, the audit scope is limited, or the auditor determines that, due to significant IS control weaknesses, it is not necessary to assess the effectiveness of all relevant IS controls. Within each relevant control activity, the auditor should identify control techniques implemented by the entity and determine whether the control techniques, as designed, are sufficient to achieve the control activity, considering IS audit risk and the audit objectives. The auditor may be able to determine whether control techniques are sufficient to achieve a particular control activity without evaluating and testing all of the control techniques. Also, depending on IS audit risk and the audit objectives, the nature and extent of control techniques necessary to achieve a particular control objective will vary.

If sufficient, the auditor should determine whether the control techniques are implemented (placed in operation) and are operating effectively. Also, the auditor should evaluate the nature and extent of testing performed by the entity. Such information can assist in

Exposure Draft

identifying key controls and in assessing risk, but the auditor should not rely on testing performed by the entity in lieu of appropriate auditor testing. If the control techniques implemented by the entity, as designed, are not sufficient to address the control activity, or the control techniques are not effectively implemented as designed, the auditor should determine the effect on IS controls and the audit objectives.

This FISCAM section includes information that should be included in audit documentation. In addition to this documentation, as discussed in FAM Sections 390 and 395H, the auditor documents relevant controls in the SCE form or equivalent documentation. Based on such controls and the audit planning procedures (particularly the identification of critical control points), the auditor should identify those other IS controls (general, business process application, interface, and data management system controls) upon which the controls in the SCE depend. FISCAM Appendices II and III can be used to document such controls.

Determine the Nature, Timing, and Extent of Control Tests

FAM Section 350 discusses determining the nature, extent, and timing of control tests and compliance with FFMIA. FAM Section 350.01 states that for each control objective, the auditor should

- identify specific relevant control activities to test (FAM 350.06-.08),
- perform walk-throughs to determine whether those controls have been placed in operation (FAM 350.09),
- document these control activities in the SCE worksheet or equivalent (FAM 350.10),
- determine the nature of control tests (FAM 350.11-.18),
- determine the extent of control tests (FAM 350.19-.20), and
- determine the timing of control tests (FAM 350.21).

As discussed in FAM Section 350, for each control objective identified in FAM 330, the auditor should identify the control activity, or combination of control activities, that is likely to (1) achieve the control objective and (2) improve the efficiency of control tests. In doing this, the auditor should consider (1) the extent of any inherent risk and control environment, risk

Exposure Draft

assessment, communication, or monitoring weaknesses, including those related to IS controls (as documented in the ARA and/or audit strategy document, or equivalent (see FAM 260)), and (2) the tentative determination of the likelihood that IS controls will be effective, as determined in the planning phase (see FAM 270). The auditor generally should test only the control activities necessary to achieve the objective.

If, in any phase of the audit, the auditor determines that control activities selected for testing are, in fact, ineffective in design or operation, the auditor should discontinue the specific control evaluation of the related control objectives and should report the identified weaknesses in internal control as discussed in FAM 580. This would include situations where the control activities are not effective in design or operation due to ineffective IS controls. If the entity's management does not agree with the auditor's conclusion that effective control activities do not exist or are unlikely to exist, the auditor may need to perform procedures sufficient to support that conclusion.

As discussed in FAM Section 350.10, the auditor should document the control activities to be tested on the SCE worksheet or equivalent (see an illustration in FAM 395 H). The auditor generally should test other components of internal control by observation and inquiry in the planning phase (see FAM 260.09). The auditor may list (and evaluate) controls that satisfy more than one control objective only once and refer to these controls, when applicable, on subsequent occasions. For each control to be tested, the auditor should determine whether the control is an IS control. An IS controls specialist generally should review and concur with the auditor's identification of IS controls.

For every IS control identified above and included in the SCE form or equivalent document, based upon IS controls audit planning, the IS controls specialist should identify the general controls (entitywide, and system levels) and business process application level controls upon which the IS controls depend. Such systems and business process application level controls would principally relate to the critical control points. For example, if the IS control is the review of an exception report, the auditor should identify and test the business process application controls directly related to the

Exposure Draft

production of the exception report, as well as the general and other business process application controls upon which the reliability of the information in the exception report depends, including the proper functioning of the business process application that generated the exception report and the reliability of the data used to generate the exception report. In addition, the auditor should test the effectiveness of the user control (i.e., management review and followup on the items in the exception report).

Test Information System Controls

FAM Section 360 discusses tests of application controls and user controls. As discussed in FAM Section 360.10, the auditor, with IS controls specialist assistance, generally should perform tests of those application controls and user controls necessary to achieve the control objectives where the entitywide, system, and application-level general controls were determined to be effective.

FAM 360.01 states that the auditor should design and conduct tests of control activities that are effective in design to determine their effectiveness in operation. (See FAM 380.02 if control activities are not effective in design during the entire audit period.) The auditor generally should

- request IS controls specialist assistance and test IS controls (FAM 360.03-.10),
- perform nonsampling control tests (the auditor generally should perform sampling control tests in the testing phase, as discussed in FAM 450), (FAM 360.11-.13), and
- evaluate the results of nonsampling control tests (FAM 360.14-.15).

If the auditor identifies IS controls for testing, the auditor, with IS controls specialist assistance, should evaluate the effectiveness of relevant

- general controls at the entitywide and system level;
- general controls at the business process application level; and
- specific business process controls, interface controls, data management system controls and/or user controls, unless the IS controls that achieve the control objectives are general controls.

Exposure Draft

If controls are not effective, see FAM 360.07 and FAM 360.09.

It is generally more efficient for the auditor to test IS controls on a tiered basis, starting with the general controls at the entitywide and system levels, followed by the general controls at the business process application level, and concluding with tests of business process application, interface, and data management system controls at the business process application level. Such a testing strategy may be used because ineffective IS controls at each tier generally preclude effective controls at the subsequent tier.

The auditor, with IS controls specialist assistance, should determine whether relevant entitywide and system level general controls are effectively designed, implemented, and operating effectively by

- identifying applicable general controls;
- determining how those controls function, and whether they have been placed in operation; and
- evaluating and testing the effectiveness of the identified controls.

The auditor and the IS controls specialist generally should use knowledge obtained in the planning phase. The auditor, with assistance from the IS controls specialist, should document the understanding of general controls and should conclude whether such controls are effectively designed, placed in operation, and, for those controls tested, operating as intended.

Tests of General Controls at the Entitywide and System Levels

The auditor may test general controls through a combination of procedures, including observation, inquiry, inspection (which includes a review of documentation on systems and procedures), and reperformance using appropriate test software. Although sampling is generally not used to test general controls, the auditor may use sampling to test certain controls, such as those involving approvals.

If general controls are not effectively designed and operating as intended, the auditor will generally be unable to obtain satisfaction that application controls are effective. In such instances, the auditor should (1) determine and document the nature and extent of risks

Exposure Draft

resulting from ineffective general controls and (2) identify and test any manual controls that achieve the control objectives that the IS controls in the SCE or equivalent document were to achieve.

However, if manual controls do not achieve the control objectives, the auditor, with IS controls specialist assistance, should determine whether any specific IS controls are designed to achieve the objectives. If not, the auditor should develop appropriate findings principally to provide recommendations to improve internal control. If specific IS controls are designed to achieve the objectives, but are in fact ineffective because of poor general controls, testing would typically not be necessary, except to support findings.

Tests of General Controls at the Business Process Application Level

If the auditor reaches a favorable conclusion on general controls at the entitywide and system levels, the IS controls specialist should evaluate and test the effectiveness of general controls for those business process applications within which business process application controls or user controls are to be tested.

If general controls are not operating effectively within the application, application controls and user controls generally will be ineffective. In such instances, the IS controls specialist should discuss the nature and extent of risks resulting from ineffective general controls with the audit team. The auditor should determine whether to proceed with the evaluation of application controls and user controls.

Tests of Business Process Application Controls and User Controls

The auditor, with IS controls specialist assistance, generally should perform tests of those business process application controls (business process controls, interface controls, and data management system controls), and user controls necessary to achieve the control objectives where the entitywide, system, and application-level general controls were determined to be effective.

Exposure Draft

As discussed in FAM Section 360.13, the auditor should test segregation of duties in the situations described in FAM 330.08. The auditor may use the following procedures to test segregation-of-duties controls:

- a. Identify the assets to be controlled through the segregation of duties.
- b. Identify the individuals who have authorized access (direct or indirect) to the assets. Direct access exists when the individual is authorized to handle the assets directly (such as during the processing of cash receipts). Indirect access exists when the individual is authorized to prepare documents that cause the release or transfer of assets (such as preparing the necessary forms to request a cash disbursement or transfer of inventory).
- c. For each individual with authorized access to assets, determine whether there are sufficient asset access controls. Asset access controls are those controls that are designed to provide assurance that actions taken by individuals with authorized access to assets are reviewed and approved by other individuals. For example, an approval of an invoice for payment generally provides asset access controls (relating to cash) over those individuals authorized to prepare supporting documentation for the transaction. If IS controls provide access to assets, the auditor should design tests of IS controls to identify (1) individuals (including IT personnel) who may use the computer to obtain access and (2) asset access controls over such individuals.
- d. For individuals with authorized access to assets over which asset access controls are insufficient, determine whether such individuals can affect any recording of transactions in the accounting records. If so, segregation of duties is insufficient, unless such access to accounting records is controlled. For example, the person who processes cash receipts may also be able to record entries in the accounting records.

Such a person may be in a position to manipulate the accounting records to conceal a shortage in the cash account, unless another individual reviews all accounting entries made (and those that should have been made) by that person. In an IT accounting system, access to assets frequently provides access to records. For example,

Exposure Draft

generation of a check may automatically record a related accounting entry. In such circumstances, a lack of asset access controls would result in inadequate segregation of duties, and the auditor should determine whether other controls would mitigate the effects of this lack of asset access control.

The FISCAM section “Test Information System Controls” included in section 2.2 provides more specific guidance on how the auditor tests relevant IS control techniques. This FISCAM section includes information that should be included in audit documentation. In addition, FISCAM Chapters 3 and 4 provide general controls and business process application level controls consistent with GAGAS categories. In addition, Appendices II and III may be used to document the results of the IS controls audit tests.

As discussed in FAM Section 390, the auditor should document the evaluation of specific control activities in the SCE worksheet or equivalent. The auditor should document control tests in the control test audit plan (formerly referred to as the audit program) and in accompanying documents. The auditor should also document any IT system control tests as discussed in FAM 370.05. FAM 395 H presents an example of a completed SCE worksheet documents. FISCAM Appendices II and III can be used to document such controls.

REPORTING THE RESULTS OF THE IS CONTROLS AUDIT

FAM Sections 370 and 580 discuss the auditor’s assessment of the effectiveness of IS controls based on internal control tests performed.

As discussed in FAM Section 370.03, based on the procedures performed, the auditor and IS controls specialist should discuss conclusions on the effectiveness of IS controls and reach agreement. The auditor should (1) incorporate the conclusions into the audit documentation for each IS control tested and (2) perform tests of application controls (principally manual follow-up of exceptions) or user controls identified by the IS controls specialist for the audit team to test.

Exposure Draft

If the auditor and the IS controls specialist determine that IS controls are effective, the auditor may also ask the IS controls specialist to identify any IS controls within the applications tested that were not previously identified by the auditor using the above procedures. For example, such IS controls might achieve control objectives not otherwise achieved through manual controls or might be more efficient or effective to test than manual controls. The IS controls specialist may assist the auditor in determining the efficiency and effectiveness of searching for and testing additional IS controls. The auditor should document these decisions, including a description of the expected scope of the IS controls specialist's work.

The auditor and the IS controls specialist should work together to document the procedures for evaluating and testing the effectiveness of IS controls and the results of this work.

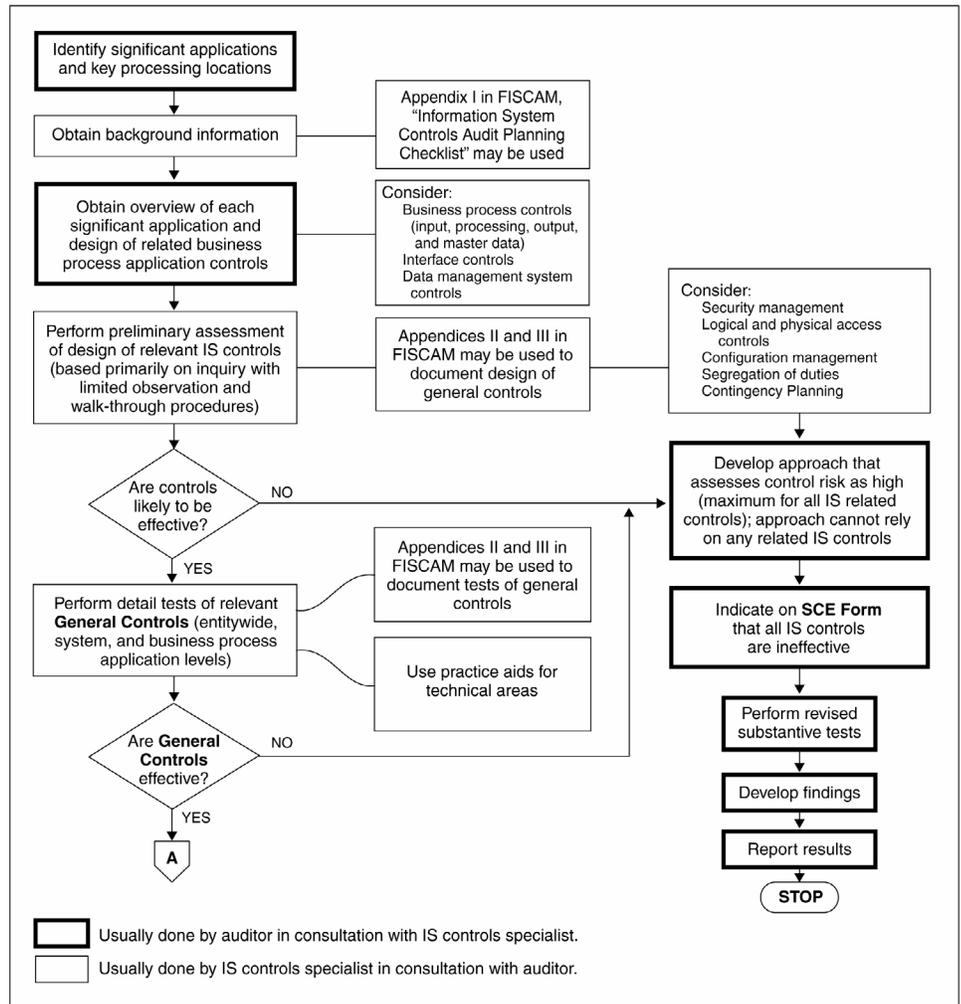
The FISCAM section 2.3 "Report Audit Results" provides more specific guidance on how the auditor evaluates the results of tests of IS controls within the context of a financial audit. More specifically, the section discusses the auditor's considerations for determining whether IS control weaknesses are material weaknesses, significant deficiencies, and significant deficiencies for purposes of FFMLA reporting.

Steps in Assessing Information System Controls

As discussed in FAM 270, the following flowcharts illustrate steps the auditor and the IS controls specialist generally follow in assessing IS controls in a financial statement audit. However, the audit team may decide to test the effectiveness of the general controls even if they are not likely to be effective (see fig. 6) or review business process application controls even though general controls are not effective (see fig. 7), in order to make recommendations on how to fix weak controls.

Exposure Draft

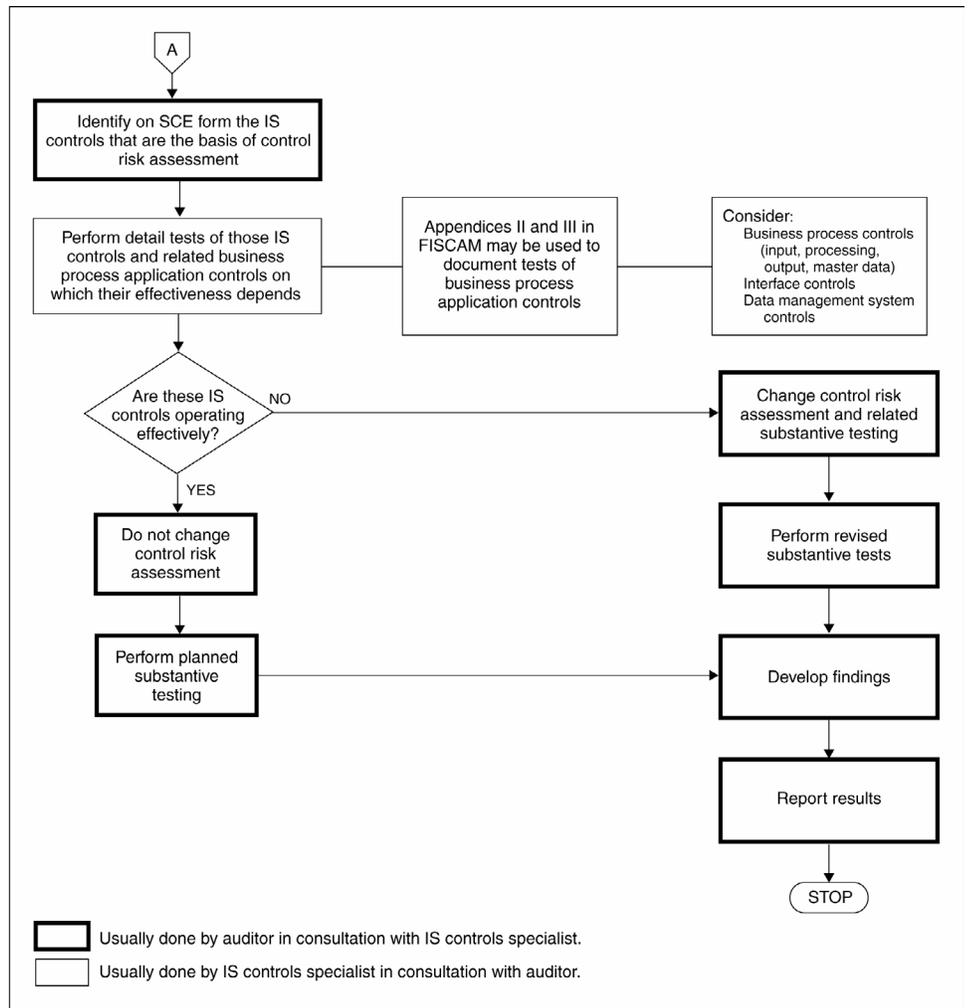
Figure 6: Steps in Assessing IT Systems Controls in a Financial Statement Audit



Source: GAO.

Exposure Draft

Figure 7: Steps for Each Significant Application in Assessing Information System Controls in a Financial Statement Audit



Source: GAO.

Exposure Draft

Appendix VII - Entity's Use of Service Organizations

Many entities use outside service organizations to support business processes. Service organizations provide services ranging from performing a specific task (e.g., payroll processing) to replacing entire business units or functions of an entity. To determine the significance of the functions performed by service organizations to the audit objectives, auditors should obtain information about (1) services performed by the service organizations, (2) the related service organization controls, and (3) their effects on the audit objectives.

If an organization uses a service organization, information and information processing are subjected to controls that may be physically and operationally removed from the user organization. Consequently, an entity's internal control may include controls that are not directly administered by the user organization, but rather by the service organization. For this reason, to obtain an understanding of IS controls, the auditor of the user organization (the user auditor) should gain an understanding of controls at the service organization that may affect the user organization's business processes. This understanding may be gained in several ways, including discussions with management and/or obtaining a service auditor's report. In addition, FISMA requirements specifically apply to information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of the entity.

During the planning stage of the audit, the user auditor should determine the significance of the service organization's controls to the user organization's internal control and to the audit objectives. Factors that may affect the significance to the audit of a service organization's controls include the following:

- The nature and materiality/significance of the transactions or information affected by the service organization

Exposure Draft

- The degree of interaction between internal control at the user organization and the service organization's controls. The degree of interaction refers to the extent to which a user organization is able to and elects to implement effective controls over the processing performed by the service organization.

With respect to financial audits, a service organization's services are part of an entity's information system, and therefore significant to the user organization's internal control, if they affect any of the following:

- The classes of transactions in the entity's operations that are significant to the financial statements
- The procedures, both automated and manual, by which the entity's transactions are initiated, recorded, processed, and reported, from their occurrence to their inclusion in the financial statements
- The related accounting records (whether electronic or manual), supporting information, and specific accounts in the financial statements involved in initiating, recording, processing, and reporting the entity's transactions
- How the entity's information system captures other events and conditions that are significant to the financial statements
- The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures

If the user auditor determines that the service organization's controls are significant to the user organization's internal control, and within the context of the audit objectives, the user auditor should gain a sufficient understanding of those controls to assess risk and plan the audit. Such controls include (1) user controls and (2) other controls implemented by the user entity to monitor the effectiveness of the design and operation of controls related to the information processed by the service organization. Such monitoring controls could include:

- contractual security requirements,
- service level agreements,

Exposure Draft

- receipt and analysis of service organization reports,
- additional testing requested of the service auditor or performed by the user entity, and
- other user entity controls

If the service organization's controls are significant to the user organization's internal control and within the context of the audit objectives, inadequate monitoring controls prevent entity management from having reasonable assurance that controls over the information processed and/or maintained by the service organization are designed and operating effectively.

Sources of information include analysis of user controls implemented by the user entity and interviews of appropriate entity personnel. Also, the auditor may review any service auditor reports. The service organization may hire an independent auditor (referred to as the service auditor) to provide a report (referred to as the SAS 70 report) on the internal controls at the service provider. Each user organization and its auditor may use this report to assess the internal control policies and procedures at the service organization as part of the overall evaluation of the internal control at the user organization. If additional information about service bureau controls is still needed, the auditor may contact the service organization, through the user entity, for additional information.

The user auditor should obtain a sufficient understanding of internal control to evaluate the effectiveness of the design of controls relevant to the audit objectives and determine whether they have been implemented. In some instances, the user entity may have effective controls over the service organization. In such cases, evidence about the operating effectiveness of internal control can be obtained from the user entity. However, in other cases, the controls are applied only at the service organization.

For internal control that is significant within the context of the audit objectives, auditors should assess whether internal control has been properly designed and implemented. Based on the user auditor's understanding of the design effectiveness and implementation of internal control, the auditor should assess risks relevant to the audit objectives. In a financial statement audit, the auditor should identify

Exposure Draft

and assess the risk of material misstatement at the financial statement level and at the relevant assertion level related to classes of transactions, account balances, and disclosures.

In a performance audit, for those internal controls that are deemed significant within the context of the audit objectives, auditors should plan to obtain sufficient, appropriate evidence to support their assessment about the operating effectiveness of those controls, including tests of such controls. In a financial audit, the auditor should perform tests of the operating effectiveness of controls when the auditor's risk assessment includes an expectation of the operating effectiveness of controls or when substantive procedures alone do not provide sufficient appropriate audit evidence at the relevant assertion level. For federal financial audits, OMB requires auditors of federal financial statements to test those controls that are effectively designed.

To obtain sufficient, appropriate evidence about the operating effectiveness of service organization controls, the auditor may determine that it is appropriate to use a service auditor's report. In such instances, the auditor should determine whether the service auditor's report is sufficient to meet the audit objectives. For financial audits, the auditor's considerations are discussed at AU 543 (Part of Audit Performed by Other Independent Auditors). In some instances, the user auditor may determine that it is necessary and appropriate to supplement the service auditor report by discussing it with the service auditor, by requesting the service auditor to perform agreed-upon procedures, or by performing procedures at the service organization. In addition, in some instances, the user auditor may request the service auditor to perform tests of data maintained by the service organizations. Any such requests of the service auditor should be coordinated through the user and service organizations.

A service auditor may provide a service organization with one of two types of SAS 70 reports:

- Type 1 is a report on the design and implementation of controls (placed in operation) at a service organization, but does not include testing of the operating effectiveness of controls. This

Exposure Draft

information, in conjunction with other information about a user organization's internal control, may assist the user auditor in obtaining an understanding of the user organization's internal control. A type 1 report is not intended to provide a basis for the auditor to reduce the assessment of risk, because it does not include control testing to determine whether the controls are operating effectively.

- Type 2 is a report on the design and implementation of controls (placed in operation) *and* on their operating effectiveness. In a type 2 engagement, the service auditor performs the procedures required for a type 1 engagement and also performs tests of specific controls to evaluate their operating effectiveness in achieving the specified control objectives. The service auditor issues a report that includes the type 1 report opinions and refers the reader to a description of tests of operative effectiveness performed by a service auditor. The report states whether, in the opinion of the service auditor, the controls tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified. If a service organization's controls that affect a user organization's financial statements are operating with sufficient effectiveness to achieve the related control objectives, a user auditor may be able to use the type 2 report as evidence of control effectiveness, reduce their assessment of risk for certain financial statement assertions affected by the service organization's service, and reduce the extent of substantive procedures performed for those assertions.

The nature, timing, and extent of the tests of operating effectiveness are also affected by the period covered by the report. Tests of operating effectiveness may provide evidence that will enable the service auditor to report on the entire period covered by the report. To be useful to user auditors, the report ordinarily should cover the reporting period of the user organization. If it does not cover the entire reporting period, the user auditor should evaluate the related effect on the user auditor's risk assessment and, for the period not covered by the service auditor report(s), should evaluate the adequacy of evidence about the operating effective of controls.

Exposure Draft

The service organization is responsible for identifying the internal controls that may be relevant to a user organization's internal control (description of controls). The service auditor is responsible for determining whether the description provides sufficient information for user auditors to obtain an understanding of those aspects of the service organization's controls that would have an effect on the user organization's internal control. Also, the service auditor may identify certain controls that the service organization assumes would be implemented by the user organization.

In OMB Circular A-123, Appendix A, OMB stated that an agency can leverage SAS 70 reports during the assessment. Management must determine if a Type II SAS 70 report exists and consider whether it is sufficient in scope. Agency management should look at the scope of the SAS 70 report in the context of the overall internal control assessment when considering the nature and type of other assessment activities needed outside of the SAS 70 process. A Type II SAS 70 report is required to be prepared by all federal entities that cross-service other federal entities per OMB Memorandum M-04-11, *Service Organization Audits*. In addition, the "Implementation Guide for OMB Circular A-123, Management's Responsibility for Internal Control Appendix A, Internal Control over Financial Reporting," issued by the Chief Financial Officer's Council (July 2005) provides guidance for considering service organization controls as part of the annual A-123 assessment.

FISMA applies to both (1) information collected or maintained by or on behalf of an agency and (2) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. As discussed in OMB Memoranda, as part of FISMA, agency management is responsible for ensuring that contractors (and others covered by FISMA) meet FISMA requirements, including annual testing. SAS 70 reports may provide sufficient evidence of contractor compliance. However, it may not address all of the FISMA control objectives and it may not ensure the specific systems that support the government or contract activity are actually reviewed.

Exposure Draft

Therefore, in determining whether SAS 70 reports provide sufficient evidence of contractor system FISMA compliance, it is the agency's responsibility to ensure:

- The scope of the SAS 70 audit was sufficient, and fully addressed the specific contractor system requiring FISMA review.
- The audit encompassed all controls and requirements of law, OMB policy and NIST guidance.

In addition, NIST SP 800-47 discusses additional steps agency management should implement with respect to contractors, such as an Interconnection Security Agreement (ISA) and a Memorandum of Understanding (MOU). The ISA specifies the technical and security requirements of the interconnection, and the MOU defines the responsibilities of the participating organizations.

SAS 70 reports do not include contingency planning controls, as auditing standards (AU 324) do not apply to internal control deficiencies that affect processing in future periods. However, service auditors can be requested to perform procedures to test the effectiveness of contingency planning controls and report the results of such testing to service organization management, who may in turn disclose the information and plans to correct deficiencies in the section of the SAS 70 report titled "Other Information Provided by the Service Organization."

The FISCAM can be used as a basis for performing a SAS 70 audit, using the control objectives discussed in Chapter 1.

Exposure Draft

Appendix VIII - Application of FISCAM to Single Audits⁹⁹

The FISCAM can be used to assess information system controls over compliance requirements and financial reporting in connection with a single audit. The following provides a brief introduction to single audit requirements and how the FISCAM relates to such requirements. See the Single Audit Act, as amended, OMB Circular A-133, the Compliance Supplement, and the AICPA Audit Guide: Government Auditing Standards and Circular A-133 Audits for additional information.

Single audits include opinions on the entity's financial statements, the schedule of expenditures of federal awards, and the entity's compliance with laws, regulations, and the provisions of contracts or grant agreements pertaining to federal awards that may have a direct and material effect on each of its major programs (referred to as compliance requirements). Government Auditing Standards ("yellow book") require certain audit procedures relating to internal controls over financial reporting in relation to the audit of the financial statements and the schedule of expenditures. In addition, auditors performing a single audit should obtain evidence about the effectiveness of internal control over the compliance requirements of major Federal programs.

In assessing internal control over compliance requirements and financial reporting, the auditor should evaluate whether the each of the specific control techniques that are significant to compliance

⁹⁹ The single audit is intended to provide a cost-effective audit for nonfederal entities in that one audit is conducted in lieu of multiple audits of individual programs. Such audits are performed in accordance with the Single Audit Act Amendments of 1996 and OMB Circular A-133 (*Audits of States, Local Governments, and Non-Profit Organizations*) to determine whether federal funds to nonfederal entities are expended properly.

Exposure Draft

and financial reporting is an information systems (IS) control. An IS controls specialist generally should review and concur with the audit team's identification of IS controls, particularly with respect to whether all IS controls were properly identified as such.

As discussed in Chapter 1, IS controls consist of those internal controls that are dependent on information systems processing and include general controls (entitywide, system, and business process application levels), business process application controls (input, processing, output, master file, interface, and data management system controls), and user controls¹⁰⁰ (controls performed by people interacting with information systems). General and business process application controls are always IS controls. A user control is an IS control if its effectiveness depends on information systems processing or the reliability (accuracy, completeness, and validity) of information processed by information systems. Conversely, a user control is not an IS control if its effectiveness does not depend on information systems processing or the reliability of information processed by information systems.

The FISCAM can be used to determine whether IS controls are (1) appropriately designed and implemented (placed in operation), and (2) operating effectively.

As discussed in Chapter 2, the auditor should identify and document the other entitywide, system, and business process level IS controls upon which the effectiveness of each significant IS control technique depends. These other IS controls will principally relate to the entitywide level controls and to each of the critical control points (including control dependencies) at the system and business process application levels. For example, if the IS control is the review of an exception report, the auditor should identify and test the business process application controls directly related to the production of the exception report, as well as the general and other business process application controls upon which the reliability of

¹⁰⁰ User controls are portions of controls that are performed by people interacting with IS controls. The effectiveness of user controls typically depend on the accuracy of the information produced by the IS controls.

Exposure Draft

the information in the exception report depends, including the proper functioning of the business process application that generated the exception report and the reliability of the data used to generate the exception report. In addition, the auditor should test the effectiveness of the user control (i.e., management review and followup on the items in the exception report).

The following sections address the audit procedures that should be applied in a single audit with respect to controls over (1) compliance requirements and (2) financial reporting.

Internal Control over Compliance Requirements

To evaluate internal control over compliance requirements for major programs, the auditor should:

- plan the audit and testing of internal control to support a low assessed level of control risk for the assertions relevant to the compliance requirements for each major program, and
- unless internal controls are ineffective in design, perform testing of the operating effectiveness of internal controls as planned to support a low assessed level of control risk for the assertions relevant to the compliance requirements for each major program.

When internal control over compliance requirements for a major program is ineffective in preventing or detecting noncompliance (either in design or operation), the auditor should report a significant deficiency (including whether any such condition is a material weakness), assess the related control risk at the maximum, and determine whether to apply further audit procedures to test compliance based on ineffective internal control.

In planning and performing a single audit, the auditor should:

- Identify the major programs subject to the single audit.
- Identify systems that process data for major programs.
- Determine the types of compliance requirements that are relevant to the audit (see A-133 and the *Compliance Supplement*).

Exposure Draft

- For each relevant type of compliance requirement, determine/identify the relevant control objectives (see the Compliance Supplement).
- For each relevant control objective, identify the internal control technique(s) designed/implemented by the entity to achieve the objective.
- Determine whether such control techniques are effectively designed to achieve the related control objective(s) and if so, whether they are placed in operation (implemented), including related IS controls upon which the effectiveness of the control technique depends. The auditor can use the FISCAM to assess the effectiveness of the design of IS control techniques and whether they have been implemented (placed in operation).
- For each control that is effectively designed and implemented (placed in operation), the auditor should determine whether it is effectively operating. The auditor can use the FISCAM to determine whether IS controls are effectively operating. As discussed in Chapter 2, for each IS control technique, the auditor should test the effectiveness of:
 - the specific IS control technique, and
 - the business process application and general controls upon which the effectiveness of specific IS control depends.

When the auditor assesses control risk below the maximum level, the auditor should obtain sufficient evidential matter to support that assessed level of control risk. The type of evidential matter, its source, its timeliness, and the existence of other evidential matter related to the conclusions to which it leads all bear on the degree of assurance the evidential matter provides.

Based on the tests of controls, the auditor should draw conclusions on the assessed level of control risk. The auditor should also consider the impact on the assessment of internal controls of any exceptions noted as part of the audit procedures applied to test conformance with compliance requirements. The assessment of the effectiveness of internal control over compliance in preventing or detecting noncompliance is determined in relation to each individual type of compliance requirement for each major program

Exposure Draft

or to an audit objective identified in the Compliance Supplement (e.g., controls over requirements for eligibility).

The auditor should determine whether any deficiencies in IS controls represent material weaknesses or significant deficiencies. The following definitions are provided in the draft reports on A-133 provided by the AICPA¹⁰¹:

- A *control deficiency* in an entity's internal control over compliance exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect noncompliance with a type of compliance requirement of a federal program on a timely basis.
- A *significant deficiency* is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to administer a federal program such that there is more than a remote likelihood that noncompliance with a type of compliance requirement of a federal program that is more than inconsequential will not be prevented or detected by the entity's internal control.
- A *material weakness* is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that material noncompliance with a type of compliance requirement of a federal program will not be prevented or detected by the entity's internal control.

¹⁰¹ The definitions currently in Circular A-133, based on superseded GAGAS, are as follows: Reportable conditions involve matters coming to the auditor's attention relating to significant deficiencies in the design or operation of the internal control over compliance that, in the auditor's judgment, could adversely affect the entity's ability to administer a major federal program in accordance with the applicable requirements of laws, regulations, contracts, and grants. A material weakness is a reportable condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that noncompliance with the applicable requirements of laws, regulations, contracts, and grants caused by error or fraud that would be material in relation to a major federal program being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.

Exposure Draft

The objectives of internal control pertaining to the compliance requirements for Federal programs are as follows:

- (1) Transactions are properly recorded and accounted for to:
 - (i) Permit the preparation of reliable financial statements and Federal reports;
 - (ii) Maintain accountability over assets; and
 - (iii) Demonstrate compliance with laws, regulations, and other compliance requirements;
- (2) Transactions are executed in compliance with:
 - (i) Laws, regulations, and the provisions of contracts or grant agreements that could have a direct and material effect on a Federal program; and
 - (ii) Any other laws and regulations that are identified in the compliance supplements; and
- (3) Funds, property, and other assets are safeguarded against loss from unauthorized use or disposition.

Part 6 of the *Compliance Supplement* is designed to assist non-Federal entities and their auditors in complying with these requirements by describing, for each type of compliance requirement, the objectives of internal control, and certain characteristics of internal control that, when present and operating effectively, may ensure compliance with program requirements. Part 6 cautions that the categorizations used in the Supplement may not necessarily reflect how an entity considers and implements internal control. Also, Part 6 was not designed as a checklist of required internal control characteristics. Non-Federal entities could have adequate internal control even though some or all of the characteristics included in Part 6 are not present. Further, non-Federal entities could have other appropriate internal controls operating effectively that have not been included in Part 6. Non-Federal entities and their auditors should exercise judgment in determining the most appropriate and cost effective internal control in a given environment or circumstance to provide reasonable assurance for compliance with Federal program requirements.

The characteristics of internal control in Part 6 of the *Compliance Supplement* are presented in the context of the components of

Exposure Draft

internal control discussed in *Internal Control-Integrated Framework* (COSO Report), published by the Committee of Sponsoring Organizations of the Treadway Commission. These components are consistent with the *Standards for Internal Control in the Federal Government* (Green Book).¹⁰² Part 6 describes characteristics of internal control relating to each of the five components of internal control that should reasonably assure compliance with the requirements of Federal laws, regulations, and program compliance requirements.

Internal Control over Financial Reporting

In addition, the auditor should gather evidence about internal controls over financial reporting, including information system controls, as part of the financial audits of the financial statements and schedule of expenditures of federal awards. The auditor may use evidence gathered in connection with the testing of controls over compliance discussed above.

GAGAS financial audit standards require the auditor to obtain an understanding of internal control over financial reporting sufficient to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures. This includes performing risk assessment procedures to evaluate the design of controls relevant to an audit of financial statements and to determine whether they have been implemented. In obtaining this understanding, the auditor considers how an entity's use of information technology (IT) and manual procedures affect controls relevant to the audit. The FISCAM can be used to assist the auditor in obtaining an understanding of internal controls relevant to the financial statements and schedule of expenditures of federal awards.

In addition, when the auditor has determined that it is not possible or practicable to reduce the detection risk at the relevant assertion level to an acceptably low level with audit evidence obtained only

¹⁰² Standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1, November 1999)

Exposure Draft

from substantive procedures, the auditor should perform tests of controls to obtain audit evidence about their operating effectiveness. For example, the auditor may find it impossible to design effective substantive procedures that by themselves provide sufficient appropriate audit evidence at the relevant assertion level when an entity conducts its business using information technology (IT) and no documentation of transactions is produced or maintained, other than through the IT system.

Specifically, as discussed in Chapter 2, for those internal controls over financial reporting that the auditor (1) has determined are suitably designed and implemented (2) plans to test whether they are operating effectively, and (3) has determined to be IS controls (as defined above), the auditor should test the effectiveness of

- the specific IS control, and
- the business process application and general controls upon which the effectiveness of specific IS control depends.

The FISCAM can be used to assess the effectiveness of the design and operation of information system controls as part of the financial audits of the financial statements and schedule of expenditures of federal awards.

Exposure Draft

Appendix IX - Application of FISCAM to FISMA

The FISCAM may be used as a basis for the independent evaluation of a federal agency's information security program required by the Federal Information Security Management Act (FISMA). A FISMA evaluation does not require an audit or the use of the FISCAM. Also, this guidance may be used to perform FISMA evaluations that are not based on GAGAS audits. For FISMA evaluations not performed as GAGAS audits, auditor judgment can be used to determine the appropriate level of documentation. This section provides guidance on how the FISCAM can be used as the basis for a FISMA evaluation.

Background

FISMA requires that each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices (see Appendix X – FISMA legislation). Each evaluation shall include:

- testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;
- an assessment (made on the basis of the results of the testing) of compliance with the requirements of FISMA; and related information security policies, procedures, standards, and guidelines; and
- separate presentations, as appropriate, regarding information security relating to national security systems.

The independent annual evaluation for non-national security systems is to be performed (1) for each agency with an Inspector General appointed under the Inspector General Act of 1978, by the Inspector General or an independent external auditor, as determined by the Inspector General of the agency; or (2) for those agencies without an inspector general, by an independent external auditor engaged by the head of the agency. For each agency

Exposure Draft

operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed (1) only by an entity designated by the agency head; and (2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

The annual independent evaluation section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency. Each year, the head of each agency shall submit to the Director of OMB the results of the evaluation. To the extent an evaluation directly relates to a national security system, the evaluation results submitted to the Director of OMB shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system. Agencies and auditors shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with risk and comply with all applicable laws and regulations.

Scope of Evaluation Procedures

As noted above, the independent evaluation shall include testing the effectiveness of information security policies, procedures, and practices for a representative subset of agency information systems. The concept of a representative subset was intended to provide the auditor (the party performing the independent evaluation) with a reasonable basis for their evaluation. The auditor should select the subset of systems for testing with the expectation that it would be representative of all of the entity's systems covered by FISMA, in all significant respects. Using professional judgment, the auditor should identify a sufficient scope of systems testing to constitute a representative subset of the entity's systems. The auditor may supplement systems tested for other purposes (e.g., financial audits) with additional systems necessary to obtain a representative subset. The auditor also may select a representative subset of systems for FISMA and supplement it with additional systems necessary to perform the financial audit or other audits. In planning the information security testing for FISMA, the auditor should perform

Exposure Draft

the following steps to identify a representative subset of agency systems:

- Understand the agency's systems – The auditor should obtain a sufficient understanding of the entity's systems (including the use of contractors and others to process information and/or to operate systems for or on behalf of the entity) to plan the evaluation so that it incorporates a representative subset of entity systems. The IS audit planning phase discussed in Chapter 2 provides a framework for understanding the entity's systems.
- Consider other information security testing – The auditor should identify information security testing that has been or will be performed during the fiscal year for which the evaluation is being performed. The auditor's evaluation should incorporate the results of this testing and should, to the extent possible, use such testing as a basis for the evaluation. For example, testing associated with the entity's financial audit can be used to support the independent evaluation. The evaluation can consider the results of multiple evaluations. In considering testing performed by parties other than the auditor, the auditor should consider the competence, independence, and objectivity of the other parties. (see below)

In determining a representative subset of agency systems, the auditor should consider the risk level of the systems, as presented in NIST Federal Information Processing Standards Publication (FIPS PUB) 199, entitled "Standards for Security Categorization of Federal Information and Information Systems". The auditor generally should test some component of high risk systems annually. In addition, a mix of moderate and low risk, major general support systems and major applications generally should be tested annually to ensure adequate coverage of all systems are performed over time. A representative subset generally would include a combination of:

- systems at different risk levels (high, moderate, and low)
- both general support systems and major application systems
- different types of applications (e.g., financial management, operations) operated by the agency
- major processing locations

Exposure Draft

- general and business process controls, including all of the control areas.
- contractor and other non-entity systems that are covered by FISMA requirements. The auditor should consider related IS controls to be significant to the user organization’s internal control and follow the procedures discussed in Appendix VII “Entity’s Use of Service Organizations.”)

In determining the specific systems to be tested in the current evaluation period, the auditor may consider recent testing performed as part of a multi-year testing strategy. Also, evidence of continuing material weaknesses or significant deficiencies may reduce the extent of testing necessary to reasonably conclude that information security is ineffective; however, the auditor should consider the benefits of testing to identify additional weaknesses that the agency can begin to address

FISMA requires that an independent evaluation be performed. This means that the auditor should be independent of the entity in fact and in appearance. In addition, if the auditor would like to use the work of other parties as a basis for the auditor’s evaluation, the auditor should consider the independence and objectivity of the persons performing the testing on behalf of the agency. If such other parties are considered independent, the auditor may determine that the work of the other parties can be used as support for the evaluation without retesting. The less independent or objective the other parties’ work is, the less the auditor can use the work of the other party without retesting the other parties’ work. If the other parties are not independent, the auditor should not use such work as a substitute for their own testing. Although GAGAS is not required to be applied in the FISMA evaluation, such standards provide guidance on considering independence that is consistent with other discussions of independence in professional literature. Also, the auditor may elect to perform the FISMA evaluation using GAGAS.

Exposure Draft

Evaluating the Results of Testing

The FISCAM was designed as a risk-based methodology to assess the effectiveness of an entity's information system controls. It can also be used to assess to provide a reasonable basis for determining whether information security is effective, and identifying information security strengths and weaknesses as a basis for that determination. The FISCAM control activities are consistent with and have been mapped to the NIST guidance (see Appendix IV).

The Reporting phase discussed in Chapter 2 describes how to evaluate the results of the tests of controls and conclude as to their effectiveness. In evaluating the results of the testing, the auditor should determine whether any weaknesses identified, individually or collectively, represent significant deficiencies as that term is used in FISMA (see "Related Reporting Responsibilities" in Chapter 2 for further information.) FISMA requires agencies to report any significant deficiencies 1) as material weaknesses under FMFIA, or 2) as instances of a lack of substantial compliance under FFMIA, if related to financial management systems. Also, the auditor should determine whether the significant deficiencies collectively result in ineffective information security controls.

OMB defines a FISMA significant deficiency as "a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems which significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken."

The following points provide guidance in applying the FISCAM to determine whether there is a FISMA significant deficiency:

- ineffective controls over any one of the nine control areas represent a FISMA significant deficiency,
- ineffective controls over one or more critical elements represent a FISMA significant deficiency unless, based upon the facts and circumstances, the auditor believes that other factors sufficiently mitigate the effect of the control weaknesses, and

Exposure Draft

- individual weaknesses or any combination of weaknesses that meet the above definition represent FISMA significant deficiencies.

Consistent with the IS audit methodology described in Chapter 2, for each FISCAM critical element, the auditor should make a summary determination as to the effectiveness of the entity's related controls based on the representative subset, considering entitywide, system, and business process application levels collectively. If the controls for one or more of each control area's critical elements are ineffective, then the controls for the entire control area are not likely to be effective. The auditor should use professional judgment in making such determinations.

Also, the auditor should evaluate the risk that the aggregate combination of weaknesses could result in unauthorized access to key systems or files. For example, a series of weaknesses might result in an individual having the ability to gain unauthorized external access to agency systems, escalate their privileges to obtain root access to critical network nodes, and consequently to key systems or files.

Further, in evaluating the results of the tests performed, the auditor should consider several factors, including:

- The likelihood that an individual could obtain unauthorized access to or perform unauthorized or inappropriate activities on key entity systems or files that could affect the confidentiality, integrity, and availability of the agency's information and information systems. This might include (1) the ability to obtain root access to system(s) that house key information or system resources (including supporting systems), thereby enabling an individual to read, add, delete, or modify data either directly or through the introduction of unauthorized software; (2) the ability to directly access and modify file(s) related to key areas of audit interest; or (3) the ability to assign unauthorized application user rights, thereby being enabled to enter unauthorized transactions or perform unauthorized activities.
- The nature of unauthorized access that could be obtained (e.g., limited to system or application programmers or system

Exposure Draft

administrators; authorized system users; or anyone through unauthorized external access through the Internet).

- The likelihood that other controls, including application controls, would prevent or detect such unauthorized access. Generally, if the effectiveness of such other controls depends on computer processed information, it is unlikely that they could effectively prevent or detect such access, unless the identified weaknesses could not reasonably result in the ability to compromise such other controls.
- The risk that management could override controls (such as through excessive access rights).

Although rare, the entity may have overall compensating controls or other factors that would mitigate or reduce the risks arising from control weaknesses. For example, manual reviews of support for all disbursements could mitigate information security risks related to a disbursement system. The auditor should determine whether there are any such compensating controls or other factors. If present, the auditor should document such controls or factors, test them appropriately to determine whether they effectively mitigate the identified information security weaknesses, and draw conclusions about the nature and extent of the risks that remain after considering such controls or factors.

If there are no significant deficiencies, the auditor may conclude that information security controls are effective for the subset tested. If there are one or more FISMA significant deficiencies, and therefore FMFIA material weaknesses, the auditor should determine whether the weaknesses, in the aggregate, are severe or pervasive, such that information security is ineffective. For example, an agency has effective controls over all of the FISCAM control areas, except for contingency planning, for which the agency has not adequately tested their contingency plans for all of the tested systems. The auditor might conclude that this FISMA significant deficiency is not sufficiently severe or pervasive to render information security ineffective. In such instances, the auditor may conclude that information security controls are effective, except for the FISMA significant deficiencies. In making this determination, the auditor should consider whether an “except for” conclusion would be misleading to a reasonable person reading the evaluation results. If

Exposure Draft

there are one or more FISMA significant deficiencies and the auditor determines that an “except for” conclusion is inappropriate, the auditor should deem information security to be ineffective.

In addition to reporting on the effectiveness of information security controls, the auditor should determine whether information used in management reports or used to support FISMA reporting to OMB is consistent with the results of the testing performed. More specifically, for each system tested, the auditor should compare the results of testing with related information included in management and FISMA reports. For example, the auditor should compare evidence obtained about a system’s certification and accreditation with information included in management and FISMA reports to determine whether such reporting was accurate (e.g., whether a certification and accreditation was completed). If, in this circumstance, a certification and accreditation was complete and was reported as such in management and FISMA reports, but the auditor’s testing revealed that it was not properly performed, the auditor should consider this deficiency in their evaluation of the results of testing and determine whether there are systemic reasons for the deficiency.

To meet the requirements of FISMA, the auditor should report on their annual independent evaluation of the effectiveness of information security for the representative subset of systems. Such report should include:

- The overall conclusion on their assessment of effectiveness of information security controls, based on testing performed,
- The significant deficiencies identified, and
- A general discussion of the nature and extent of testing performed.

Such report should be in addition to other OMB reporting requirements.

However, as discussed above, (1) such reporting directly related to a national security system shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system, and (2) agencies and auditors shall take

Exposure Draft

appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security.

For additional guidance on performing FISMA evaluations, refer to the PCIE FISMA Framework.

Exposure Draft

Appendix X - Federal Information Security Management Act of 2002 (FISMA)

P.L. 107-347, Title III, sec. 301-305, December 17, 2002

TITLE III--INFORMATION SECURITY

Sec. 301. INFORMATION SECURITY.

(a) Short Title.--This title may be cited as the "Federal Information Security Management Act of 2002".

(b) Information Security.--

(1) In general.-- Chapter 35 of title 44, United States Code, is amended by adding at the end the following new subchapter:

"SUBCHAPTER III--INFORMATION SECURITY

"Sec. 3541. Purposes

"The purposes of this subchapter are to--

"(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

"(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

Exposure Draft

"(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

"(4) provide a mechanism for improved oversight of Federal agency information security programs;

"(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and

"(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

"Sec. 3542. Definitions

"(a) In General.--Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

"(b) Additional Definitions.--As used in this subchapter:

"(1) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide--

"(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

"(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

"(C) availability, which means ensuring timely and reliable access to and use of information.

Exposure Draft

"(2)(A) The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency--

"(i) the function, operation, or use of which--

"(I) involves intelligence activities;

"(II) involves cryptologic activities related to national security;

"(III) involves command and control of military forces;

"(IV) involves equipment that is an integral part of a weapon or weapons system; or

"(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

"(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

"(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

"(3) The term 'information technology' has the meaning given that term in section 11101 of title 40.

"Sec. 3543. Authority and functions of the Director

"(a) In General.--The Director shall oversee agency information security policies and practices, including--

"(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and

Exposure Draft

compliance with standards promulgated under section 11331 of title 40;

"(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of--

"(A) information collected or maintained by or on behalf of an agency; or

"(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

"(3) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

"(4) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements;

"(5) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3544(b);

"(6) coordinating information security policies and procedures with related information resources management policies and procedures;

"(7) overseeing the operation of the Federal information security incident center required under section 3546; and

Exposure Draft

"(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including--

"(A) a summary of the findings of evaluations required by section 3545;

"(B) an assessment of the development, promulgation, and adoption of, and compliance with, standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) and promulgated under section 11331 of title 40;

"(C) significant deficiencies in agency information security practices;

"(D) planned remedial action to address such deficiencies; and

"(E) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(d)(10) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

"(b) National Security Systems.--Except for the authorities described in paragraphs (4) and (8) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

"(c) Department of Defense and Central Intelligence Agency Systems.--(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of Central Intelligence in the case of systems described in paragraph (3).

"(2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

Exposure Draft

"(3) The systems described in this paragraph are systems that are operated by the Central Intelligence Agency, a contractor of the Central Intelligence Agency, or another entity on behalf of the Central Intelligence Agency that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Central Intelligence Agency.

"Sec. 3544. Federal agency responsibilities

"(a) In General.—The head of each agency shall—

"(1) be responsible for—

"(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

"(i) information collected or maintained by or on behalf of the agency; and

"(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

"(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

"(i) information security standards promulgated under section 11331 of title 40; and

"(ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

"(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

Exposure Draft

"(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through--

"(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

"(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;

"(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

"(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

"(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including--

"(A) designating a senior agency information security officer who shall--

"(i) carry out the Chief Information Officer's responsibilities under this section;

"(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

"(iii) have information security duties as that official's primary duty; and

Exposure Draft

"(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

"(B) developing and maintaining an agencywide information security program as required by subsection (b);

"(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3543 of this title, and section 11331 of title 40;

"(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

"(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

"(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

"(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

"(b) Agency Program.--Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes--

"(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

Exposure Draft

"(2) policies and procedures that--

"(A) are based on the risk assessments required by paragraph (1);

"(B) cost-effectively reduce information security risks to an acceptable level;

"(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

"(D) ensure compliance with--

"(i) the requirements of this subchapter;

"(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;

"(iii) minimally acceptable system configuration requirements, as determined by the agency; and

"(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

"(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

"(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of--

"(A) information security risks associated with their activities; and

"(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

"(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be

Exposure Draft

performed with a frequency depending on risk, but no less than annually, of which such testing--

"(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and

"(B) may include testing relied on in a evaluation under section 3545;

"(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

"(7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including--

"(A) mitigating risks associated with such incidents before substantial damage is done;

"(B) notifying and consulting with the Federal information security incident center referred to in section 3546; and

"(C) notifying and consulting with, as appropriate--

"(i) law enforcement agencies and relevant Offices of Inspector General;

"(ii) an office designated by the President for any incident involving a national security system; and

"(iii) any other agency or office, in accordance with law or as directed by the President; and

"(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Exposure Draft

"(c) Agency Reporting.--Each agency shall--

"(1) report annually to the Director, the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter, including compliance with each requirement of subsection (b);

"(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to--

"(A) annual agency budgets;

"(B) information resources management under subchapter 1 of this chapter;

"(C) information technology management under subtitle III of title 40;

"(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

"(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101-576) (and the amendments made by that Act);

"(F) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note); and

"(G) internal accounting and administrative controls under section 3512 of title 31, (known as the 'Federal Managers Financial Integrity Act'); and

"(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)--

Exposure Draft

"(A) as a material weakness in reporting under section 3512 of title 31; and

"(B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).

"(d) Performance Plan.--(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of--

"(A) the time periods, and

"(B) the resources, including budget, staffing, and training,

that are necessary to implement the program required under subsection (b).

"(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1).

"(e) Public Notice and Comment.--Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

"Sec. 3545. Annual independent evaluation

"(a) In General.--(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

"(2) Each evaluation under this section shall include--

"(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

Exposure Draft

"(B) an assessment (made on the basis of the results of the testing) of compliance with--

"(i) the requirements of this subchapter; and

"(ii) related information security policies, procedures, standards, and guidelines; and

"(C) separate presentations, as appropriate, regarding information security relating to national security systems.

"(b) Independent Auditor.--Subject to subsection (c)--

"(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

"(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

"(c) National Security Systems.--For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed--

"(1) only by an entity designated by the agency head; and

"(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

"(d) Existing Evaluations.--The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

Exposure Draft

"(e) Agency Reporting.--(1) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

"(2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

"(f) Protection of Information.--Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

"(g) OMB Reports to Congress.--(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3543(a)(8).

"(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

"(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of Central Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

"(h) Comptroller General.--The Comptroller General shall periodically evaluate and report to Congress on--

"(1) the adequacy and effectiveness of agency information security policies and practices; and

"(2) implementation of the requirements of this subchapter.

Exposure Draft

"Sec. 3546. Federal information security incident center

"(a) In General.—The Director shall ensure the operation of a central Federal information security incident center to--

"(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

"(2) compile and analyze information about incidents that threaten information security;

"(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities; and

"(4) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

"(b) National Security Systems.—Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

"Sec. 3547. National security systems

"The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency--

"(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;

Exposure Draft

"(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

"(3) complies with the requirements of this subchapter.

"Sec. 3548. Authorization of appropriations

"There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.

"Sec. 3549. Effect on existing law

"Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards and Technology Act (15 U.S.C. 278g-3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States. While this subchapter is in effect, subchapter II of this chapter shall not apply."

(2) Clerical amendment.-- The table of sections at the beginning of such chapter 35 is amended by adding at the end the following:

"SUBCHAPTER III--INFORMATION SECURITY

"Sec.

"3541. Purposes.

"3542. Definitions.

Exposure Draft

"3543. Authority and functions of the Director.

"3544. Federal agency responsibilities.

"3545. Annual independent evaluation.

"3546. Federal information security incident center.

"3547. National security systems.

"3548. Authorization of appropriations.

"3549. Effect on existing law."

(c) Information Security Responsibilities of Certain Agencies.--

(1) National security responsibilities.-- (A) Nothing in this Act (including any amendment made by this Act) shall supersede any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems, as defined by section 3542(b)(2) of title 44, United States Code.

(B) Section 2224 of title 10, United States Code, is amended--

(i) in subsection (b), by striking "(b) Objectives and Minimum Requirements.--(1)" and inserting "(b) Objectives of the Program.--";

(ii) in subsection (b), by striking paragraph (2); and

(iii) in subsection (c), in the matter preceding paragraph (1), by inserting ", including through compliance with subchapter III of chapter 35 of title 44" after "infrastructure".

(2) Atomic energy act of 1954.-- Nothing in this Act shall supersede any requirement made by or under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.). Restricted data or formerly restricted data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).

Exposure Draft

Sec. 302. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) In General.--Section 11331 of title 40, United States Code, is amended to read as follows:

"Sec. 11331. Responsibilities for Federal information systems standards

"(a) Standards and Guidelines.--

"(1) Authority to prescribe.-- Except as provided under paragraph (2), the Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3(a)), prescribe standards and guidelines pertaining to Federal information systems.

"(2) National security systems.-- Standards and guidelines for national security systems (as defined under this section) shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

"(b) Mandatory Requirements.--

"(1) Authority to make mandatory.-- Except as provided under paragraph (2), the Secretary shall make standards prescribed under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of Federal information systems.

"(2) Required mandatory standards.-- (A) Standards prescribed under subsection (a)(1) shall include information security standards that--

"(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3(b)); and

"(ii) are otherwise necessary to improve the security of Federal information and information systems.

Exposure Draft

"(B) Information security standards described in subparagraph (A) shall be compulsory and binding.

"(c) Authority to Disapprove or Modify.--The President may disapprove or modify the standards and guidelines referred to in subsection (a)(1) if the President determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

"(d) Exercise of Authority.--To ensure fiscal and policy consistency, the Secretary shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director of the Office of Management and Budget.

"(e) Application of More Stringent Standards.--The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards the Secretary prescribes under this section if the more stringent standards--

"(1) contain at least the applicable standards made compulsory and binding by the Secretary; and

"(2) are otherwise consistent with policies and guidelines issued under section 3543 of title 44.

"(f) Decisions on Promulgation of Standards.--The decision by the Secretary regarding the promulgation of any standard under this section shall occur not later than 6 months after the submission of the proposed standard to the Secretary by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

"(g) Definitions.--In this section:

Exposure Draft

"(1) Federal information system.-- The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

"(2) Information security.-- The term 'information security' has the meaning given that term in section 3542(b)(1) of title 44.

"(3) National security system.-- The term 'national security system' has the meaning given that term in section 3542(b)(2) of title 44."

(b) Clerical Amendment.--The item relating to section 11331 in the table of sections at the beginning of chapter 113 of such title is amended to read as follows:

"11331. Responsibilities for Federal information systems standards."

Sec. 303. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), is amended by striking the text and inserting the following:

"(a) In General.--The Institute shall--

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for information systems;

"(2) develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems (as defined in section 3542(b)(2) of title 44, United States Code); and

"(3) develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

Exposure Draft

"(b) Minimum Requirements for Standards and Guidelines.--The standards and guidelines required by subsection (a) shall include, at a minimum--

"(1)(A) standards to be used by all agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;

"(B) guidelines recommending the types of information and information systems to be included in each such category; and

"(C) minimum information security requirements for information and information systems in each such category;

"(2) a definition of and guidelines concerning detection and handling of information security incidents; and

"(3) guidelines developed in conjunction with the Department of Defense, including the National Security Agency, for identifying an information system as a national security system consistent with applicable requirements for national security systems, issued in accordance with law and as directed by the President.

"(c) Development of Standards and Guidelines.--In developing standards and guidelines required by subsections (a) and (b), the Institute shall--

"(1) consult with other agencies and offices and the private sector (including the Director of the Office of Management and Budget, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, and the Secretary of Homeland Security) to assure--

"(A) use of appropriate information security policies, procedures, and techniques, in order to improve information security and avoid unnecessary and costly duplication of effort; and

Exposure Draft

"(B) that such standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems;

"(2) provide the public with an opportunity to comment on proposed standards and guidelines;

"(3) submit to the Secretary of Commerce for promulgation under section 11331 of title 40, United States Code--

"(A) standards, as required under subsection (b)(1)(A), no later than 12 months after the date of the enactment of this section; and

"(B) minimum information security requirements for each category, as required under subsection (b)(1)(C), no later than 36 months after the date of the enactment of this section;

"(4) issue guidelines as required under subsection (b)(1)(B), no later than 18 months after the date of the enactment of this section;

"(5) to the maximum extent practicable, ensure that such standards and guidelines do not require the use or procurement of specific products, including any specific hardware or software;

"(6) to the maximum extent practicable, ensure that such standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks; and

"(7) to the maximum extent practicable, use flexible, performance-based standards and guidelines that permit the use of off-the-shelf commercially developed information security products.

"(d) Information Security Functions.--The Institute shall--

"(1) submit standards developed pursuant to subsection (a), along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 11331 of title 40, United States Code;

Exposure Draft

"(2) provide technical assistance to agencies, upon request, regarding--

"(A) compliance with the standards and guidelines developed under subsection (a);

"(B) detecting and handling information security incidents; and

"(C) information security policies, procedures, and practices;

"(3) conduct research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security;

"(4) develop and periodically revise performance indicators and measures for agency information security policies and practices;

"(5) evaluate private sector information security policies and practices and commercially available information technologies to assess potential application by agencies to strengthen information security;

"(6) assist the private sector, upon request, in using and applying the results of activities under this section;

"(7) evaluate security policies and practices developed for national security systems to assess potential application by agencies to strengthen information security;

"(8) periodically assess the effectiveness of standards and guidelines developed under this section and undertake revisions as appropriate;

"(9) solicit and consider the recommendations of the Information Security and Privacy Advisory Board, established by section 21, regarding standards and guidelines developed under subsection (a) and submit such recommendations to the Secretary of Commerce with such standards submitted to the Secretary; and

Exposure Draft

"(10) prepare an annual public report on activities undertaken in the previous year, and planned for the coming year, to carry out responsibilities under this section.

"(e) Definitions.--As used in this section--

"(1) the term 'agency' has the same meaning as provided in section 3502(1) of title 44, United States Code;

"(2) the term 'information security' has the same meaning as provided in section 3542(b)(1) of such title;

"(3) the term 'information system' has the same meaning as provided in section 3502(8) of such title;

"(4) the term 'information technology' has the same meaning as provided in section 11101 of title 40, United States Code; and

"(5) the term 'national security system' has the same meaning as provided in section 3542(b)(2) of title 44, United States Code.

"(f) Authorization of Appropriations.--There are authorized to be appropriated to the Secretary of Commerce \$ 20,000,000 for each of fiscal years 2003, 2004, 2005, 2006, and 2007 to enable the National Institute of Standards and Technology to carry out the provisions of this section."

Sec. 304. INFORMATION SECURITY AND PRIVACY ADVISORY BOARD.

Section 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-4), is amended--

(1) in subsection (a), by striking "Computer System Security and Privacy Advisory Board" and inserting "Information Security and Privacy Advisory Board";

(2) in subsection (a)(1), by striking "computer or telecommunications" and inserting "information technology";

(3) in subsection (a)(2)--

Exposure Draft

(A) by striking "computer or telecommunications technology" and inserting "information technology"; and

(B) by striking "computer or telecommunications equipment" and inserting "information technology";

(4) in subsection (a)(3)–

(A) by striking "computer systems" and inserting "information system"; and

(B) by striking "computer systems security" and inserting "information security";

(5) in subsection (b)(1) by striking "computer systems security" and inserting "information security";

(6) in subsection (b) by striking paragraph (2) and inserting the following:

"(2) to advise the Institute, the Secretary of Commerce, and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, including through review of proposed standards and guidelines developed under section 20; and";

(7) in subsection (b)(3) by inserting "annually" after "report";

(8) by inserting after subsection (e) the following new subsection:

"(f) The Board shall hold meetings at such locations and at such time and place as determined by a majority of the Board.";

(9) by redesignating subsections (f) and (g) as subsections (g) and (h), respectively; and

(10) by striking subsection (h), as redesignated by paragraph (9), and inserting the following:

"(h) As used in this section, the terms 'information system' and 'information technology' have the meanings given in section 20.".

Exposure Draft

Sec. 305. TECHNICAL AND CONFORMING AMENDMENTS.

(a) Computer Security Act.--Section 11332 of title 40, United States Code, and the item relating to that section in the table of sections for chapter 113 of such title, are repealed.

(b) Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001.--The Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (Public Law 106-398) is amended by striking section 1062 (44 U.S.C. 3531 note).

(c) Paperwork Reduction Act.--(1) Section 3504(g) of title 44, United States Code, is amended--

(A) by adding "and" at the end of paragraph (1);

(B) in paragraph (2)--

(i) by striking "sections 11331 and 11332(b) and (c) of title 40" and inserting "section 11331 of title 40 and subchapter II of this chapter"; and

(ii) by striking "; and" and inserting a period; and

(C) by striking paragraph (3).

(2) Section 3505 of such title is amended by adding at the end--

"(c) Inventory of Major Information Systems.--(1) The head of each agency shall develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of such agency.

"(2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.

"(3) Such inventory shall be--

"(A) updated at least annually;

Exposure Draft

"(B) made available to the Comptroller General; and

"(C) used to support information resources management, including--

"(i) preparation and maintenance of the inventory of information resources under section 3506(b)(4);

"(ii) information technology planning, budgeting, acquisition, and management under section 3506(h), subtitle III of title 40, and related laws and guidance;

"(iii) monitoring, testing, and evaluation of information security controls under subchapter II;

"(iv) preparation of the index of major information systems required under section 552(g) of title 5, United States Code; and

"(v) preparation of information system inventories required for records management under chapters 21, 29, 31, and 33.

"(4) The Director shall issue guidance for and oversee the implementation of the requirements of this subsection."

(3) Section 3506(g) of such title is amended--

(A) by adding "and" at the end of paragraph (1);

(B) in paragraph (2)--

(i) by striking "section 11332 of title 40" and inserting "subchapter II of this chapter"; and

(ii) by striking "; and" and inserting a period; and

(C) by striking paragraph (3).

Exposure Draft

Appendix XI - Information System Controls Audit Documentation

This appendix summarizes the audit documentation that should be prepared by the auditor in connection with the IS controls audit, as discussed in Chapter 2.

Planning Phase

The auditor should document the following information developed in the planning phase:

- Objectives of the IS controls audit and, if it is part of a broader audit, a description of how such objectives support the overall audit objectives.
- The scope of the IS controls audit.
- The auditor's understanding of the entity's operations and key business processes, including, to the extent relevant to the audit objectives, the following:
 - The significance and nature of the programs and functions supported by information systems;
 - Key business processes relevant to the audit objectives, including business rules, transaction flows, and application and software module interaction;
 - Significant general support systems and major applications that support each key process;
 - Background information request, if used;
 - Significant internal and external factors that could affect the IS controls audit objectives;
 - Detailed organization chart, particularly the IT and the IS components;
 - Significant changes in the IT environment/architecture or significant applications implemented within the past 2 years or planned within the next 2 years; and

Exposure Draft

- The entity's reliance on third parties to provide IT services (e.g., in-house, remote connectivity, remote processing).
- A general understanding of the structure of the entity's or component's networks as a basis for planning the IS controls audit, including high-level and detailed network schematics relevant to the audit objectives.
- Key areas of audit interest, including relevant general support systems and major applications and files. This includes (1) the operational locations of each key system or file, (2) significant components of the associated hardware and software (e.g., firewalls, routers, hosts, operating systems), (3) other significant systems or system-level resources that support the key areas of audit interest, and (4) prior audit problems reported. Also, the auditor should document all access paths in and out of the key areas of audit interest.
- Factors that significantly increase or decrease IS risk and their potential impact on the effectiveness of information system controls. For each risk identified, the auditor should document the nature and extent of the risk; the conditions that gave rise to that risk; and the specific information or operations affected (if not pervasive).
- Preliminary assessment of IS risks related to the key areas of audit interest and the basis for the assessed risk. For each risk identified, the auditor should document the nature and extent of the risk; the conditions that gave rise to that risk; and the specific information or operations affected (if not pervasive). The auditor should also document other considerations that may mitigate the effects of identified risks.
- Critical control points.
- A preliminary understanding of the entity's IS controls, including the organization, staffing, responsibilities, authorities, and resources of the entity's security management function. The auditor should include the following information in the documentation of their preliminary understanding of the design of IS controls, to the extent relevant to the audit objectives:
 - Identification of entitywide level controls (and appropriate system level controls) designed to achieve the control activities for each critical element within each general control area and a determination of whether they are designed

Exposure Draft

effectively and implemented (placed in operation), including identification of control activities for which there are no or ineffective controls at the entitywide level and the related risks;

- Identification of business process level controls for key applications identified as key areas of audit interest, determination of where those controls are implemented (placed in operation) within the entity's systems, and the auditor's conclusion about whether the controls are designed effectively, including identification of control activities for which there are no or ineffective controls and the related risks and the potential impact of any identified design weaknesses on the completeness, accuracy, validity, and confidentiality of application data;
- Any internal or third-party information systems reviews, audits, or specialized systems testing (e.g., penetration tests, disaster recovery tests, and application-specific tests) performed during the last year;
- Management's plans of action and milestones, or their equivalent, that identify corrective actions planned to address known IS control weaknesses;
- Status of the prior years' audit findings;
- Documentation for any significant computer security related incidents identified and reported for the last year;
- Documented security plans;
- Documented risk assessments for relevant systems (e.g., general support systems and major applications);
- System certification and accreditation documentation or equivalent for relevant systems;
- Documented business continuity of operations plans and disaster recovery plans; and
- A description of the entity's use of third-party IT services
- Relevant laws and regulations and their relation to the audit objectives.
- Description of the auditor's procedures to consider the risk of fraud, any fraud risk factors that the auditor believes could affect the audit objectives, and planned audit procedures to detect any fraud significant to the audit objectives.

Exposure Draft

- Audit resources planned.
- Current multiyear testing plans.
- Documentation of communications with entity management.
- If IS controls are performed by service organizations, conclusions whether such controls are significant to the audit objectives and any audit procedures performed with respect to such controls (e.g., review of service auditor reports)
- If the auditor plans to use the work of others, conclusions concerning the planned use of the work of others and any audit procedures performed with respect to using the work of others.
- Audit plan that adequately describes the objectives, scope, and methodology of the audit.
- Any decision to reduce testing of IS controls due to the identification of significant IS control weaknesses.

Testing Phase

The auditor should document the following information developed in the testing phase:

- An understanding of the information systems that are relevant to the audit objectives
- IS control objectives and activities relevant to the audit objectives.
- By level (e.g., entitywide, system, business process application) and system sublevel (e.g., network, operating system, infrastructure applications), a description of control techniques used by the entity to achieve the relevant control activities.
- By level and sublevel, specific tests performed, including:
 - related documentation that describes the nature, timing, and extent of the tests;
 - evidence of the effective operation of the control techniques or lack thereof (e.g., memos describing procedures and results, output of tools and related analysis);
 - if a control activity is not achieved, any compensating controls or other factors and the basis for determining whether they are effective;

Exposure Draft

- the auditor's conclusions about the effectiveness of the entity's IS controls in achieving the control activity; and
- for each weakness, whether the weakness is a material weakness, significant deficiency, or just a deficiency, as well as the criteria, condition, cause, and effect if necessary to achieve the audit objectives.

Reporting Phase

The auditor should document the following information developed in the reporting phase:

- The auditor's conclusion about the effectiveness of IS controls (in relation to the IS controls audit objectives) in achieving the critical elements and the relevant control activities and the basis for the conclusion, including the factors that the auditor considered in making the determination.
- If part of a broader audit, the impact of any identified IS control weaknesses on the overall audit objectives.
- Copies of any reports or written communications issued in connection with the audit, including entity management comments related to such reports and communications.
- For financial audits and attestation engagements, the auditor's determination of whether identified weaknesses represent material weaknesses or significant deficiencies, and the basis for the auditor's conclusions.
- Other documentation required by the audit organization's policies and procedures, including quality assurance processes.
- Results of procedures to detect any fraud significant to the audit objectives and the impact on the audit.
- Results of audit follow-up procedures to determine whether agency corrective actions have been implemented, based on risk and a cost benefit analysis, to sufficiently remediate previously reported IS control weaknesses.
- As appropriate, the auditor's considerations and determinations concerning FMFIA, FFMLA, and other reporting responsibilities.

Exposure Draft

Appendix XII - Glossary

The definitions in this glossary are drawn from various sources, including this manual and the materials in the bibliography. In addition, certain definitions were developed by project staff and contractors.

Acceptance testing	Final testing by users to decide whether to accept a new system.
Access control	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).
Access control list (ACL)	A register of: 1) users (including groups, machines, and processes) who have been given permission to use a particular system resource, and 2) the types of access they have been permitted.
Access control software	(CA-ACF2, RACF, CA-TOP SECRET) This type of software, which is external to the operating system, provides a means of specifying who has access to a system, which has access to specific resources, and what capabilities authorized users are granted. Access control software can generally be implemented in different modes that provide varying degrees of protection such as denying access for which the user is not expressly authorized, allowing access which is not expressly authorized but providing a warning, or allowing access to all resources without warning regardless of authority.
Access method	The technique used for selecting records in a file for processing, retrieval, or storage.
Access path	Sequence of hardware and software components significant to access control. Any component capable of enforcing access restrictions or any component that could be used to bypass an access restriction should be considered part of the access path. The access path can also be defined as the path through which a user request travels, including the telecommunications software, transaction processing software, application program, etc.
Access path diagram	Network schematic that identifies the users of the system, the type of device from which they can access the system, the software used to access the system, the resource they may access, the system on which these resources reside, and the modes of operation and telecommunication paths.

Exposure Draft

Access privileges	Precise statements that define the extent to which an individual can access computer systems and use or modify the programs and data on a system, and under what circumstances this access will be allowed.
Access rights	Also called permissions or privileges, these are the rights granted to users by the administrator or supervisor. Access rights determine the actions users can perform (e.g., read, write, execute, create and delete) on files in shared volumes or file shares on the server.
Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
Account Management	Involves (1) the process of requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.
Accreditation	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Accreditation boundary	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected.
Accuracy	See Accuracy Control.
Accuracy control	Controls that are designed to provide reasonable assurance that transactions are properly recorded, with correct amount/data, and on a timely basis (in the proper period); key data elements input for transactions are accurate; data elements are processed accurately by applications that produce reliable results; and output is accurate.
Adequate security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Advanced Encryption Standard (AES)	The Advanced Encryption Standard specifies a U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.
Alternate work site	Entity authorized work at home or at geographically convenient satellite offices (e.g., telecommuting).

Exposure Draft

Application controls	Application controls, sometimes referred to as business controls, are incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of data during application processing and reporting.
Application level general controls	Controls consist of general controls operating at the business process application level, including those related to security management, access controls, configuration management, segregation of duties, and contingency planning.
Application System	The use of information resources to satisfy a specific set of user requirements. Performs a certain type of work, including specific functions such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application system can manipulate text, numbers, graphics, or a combination of these elements.
Application programmer	A person who develops and maintains application programs, as opposed to system programmers who develop and maintain the operating system and system utilities.
Application programs	See application system.
Assertion	Financial statement assertions are management representations that are embodied in financial statement components. The assertions can be either explicit or implicit and can be classified into the following broad categories: existence or occurrence (an entity's assets or liabilities exist at a given date and recorded transactions have occurred during a given period; completeness (all transactions and accounts that should be presented in the financial statements are included; rights and obligations (assets are the rights of the entity and liabilities are the obligations of the entity at a given date; valuation or allocation (asset, liability, revenue, and expense components have been included in the financial statements at appropriate amounts; and presentation and disclosure (the particular components of the financial statements are properly classified, described, and disclosed).
Attack	Attempt to gain unauthorized access to an information system's services, resources, or information, or the attempt to compromise an information system's integrity, availability, or confidentiality.
Audit logging	Recording of user activity in a system or application initiated by the user (e.g., access to a file, record, or field, use of modem). Further, it may record any attempts to log on (successful or unsuccessful) to a system and record log on ID, date and time of each log on.

Exposure Draft

Audit plan	A high level description of the audit work to be performed in a certain period of time (ordinarily a year). It includes the areas to be audited, the type of work planned, the high level objectives and scope of the work, and topics such as budget, resource allocation, schedule dates, type of report and its intended audience and other general aspects of the work.
Auditable event	A system activity identified by the agency's audit monitoring system that may be indicative of a violation of security policy. The activity may range from simple browsing to attempts to plant a Trojan horse or gain unauthorized access privilege.
Audit risk	For financial statement audits, the risk that the auditor may unknowingly fail to appropriately modify the audit opinion on financial statements that are materially misstated. In a performance audit, the risk that the auditor's findings, conclusions, recommendations, or assurance may be improper or incomplete.
Audit strategy	Plan for assessing organizational activities based on an understanding of the entity's business processes and related risk assessments.
Audit trail	A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.
Authorization	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Authorizing official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Availability	Ensuring timely and reliable access to and use of information.
Backdoor	An undocumented way to gain access to a program, data, or an entire computer system, often known only to the programmer who created it. Backdoors can be handy when the standard way of getting information is unavailable, but they usually constitute a security risk.

Exposure Draft

Backup	Any duplicate of a primary resource function, such as a copy of a computer program or data file. This standby is used in case of loss or failure of the primary resource.
Backup procedures	A regular maintenance procedure that copies all new or altered files to a backup storage medium, such as a tape drive.
Baseline configuration	Current inventory of all entity hardware, software, and firmware plus approved changes from the baseline.
Biometric	A physical or behavioral characteristic of a human being.
Boundary	Software, hardware, or physical barrier that limits access to a system or part of a system.
Boundary Protection	Monitoring and control of communications at the external boundary between information systems completely under the management and control of the organization, and at key internal boundaries between information systems completely under the management and control of the organization, to prevent and detect malicious and other unauthorized communication, employing controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels).
Browsing	The act of electronically perusing files and records without authorization.
Business Impact Analysis (BIA)	An analysis of an information technology (IT) system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
Business process	Processes that are the primary functions that the entity performs in accomplishing its mission. Examples include, financial management processes, such as collections, disbursements, or payroll; and mission-related processes, typically at the program or subprogram level, such as education, public health, law enforcement, or income security.
Business process application	A computer program designed to help perform a business function such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements.
Business process application controls	Controls directly related to individual computerized applications. They help ensure that transactions are complete, accurate, valid, and confidential. These controls include programmed control techniques, such as automated edits, and manual follow-up of computer generated reports, such as reviews of reports identifying rejected or unusual items.
Business process application level	Controls at the business process application level consist of policies, procedures for controlling specific processes. For example, the entity's configuration management should reasonably ensure that all changes to application systems are fully tested and authorized.

Exposure Draft

Business process controls (FISCAM)	These controls are the automated and /or manual controls applied to business transaction flows. They relate to the completeness, accuracy, validity and confidentiality of transactions and data during application processing.
Bypass label processing (BLP)	The technique of reading a computer file while bypassing the internal file/data set label. This process could result in bypassing security access controls.
CAAT	See computer-assisted audit technique.
CD-ROM	See compact disk-read only memory.
Central processing unit (CPU)	The computational and control unit of a computer; the device that interprets and executes instructions.
Certificate	A digital representation of information which at least 1) identifies the certification authority issuing it, 2) names or identifies its subscriber, 3) contains the subscriber's public key, 4) identifies its operational period, and 5) is digitally signed by the certification authority issuing it.
Certificate Authority (CA)	A trusted third party that serves authentication infrastructures or organizations and registers entities and issues them certificates.
Certificate Management	Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed.
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Certification and Accreditation	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Certification Authority	A trusted entity that issues and revokes public key certificates.

Exposure Draft

Checkpoint	The process of saving the current state of a program and its data, including intermediate results, to disk or other nonvolatile storage, so that, if interrupted, the program could be restarted at the point at which the last checkpoint occurred.
Chief Information Officer	Agency official responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, information policies and information resources management responsibilities, including information security and the management of information technology.
Cipher key lock	A lock with a key pad-like device that requires the manual entry of a predetermined code for entry.
Cipher text	Data output from the Cipher or input to the Inverse Cipher. Data in its encrypted form.
Code	Instructions written in a computer programming language. (See object code and source code.)
Cold site	An IS backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternative site.
Collaborative computing	Applications and technology (e.g., white boarding, group conferencing) that allow two or more individuals to share information real time in an inter- or intra-enterprise environment.
Command	A job control statement or a message, sent to the computer system, that initiates a processing task.
Compact disc-read only memory (CD-ROM)	Compact Disc (CD)-Read Only Memory (ROM) is a form of optical, rather than magnetic, storage. CD-ROM devices are generally read only.
Compensating control	An internal control that reduces the risk of an existing or potential control weakness that could result in errors or omissions.
Compiler	A program that reads the statements in a human-readable programming language and translates them into a machine-readable executable program.
Completeness control	Controls that ensure entity management that all transactions that occurred are entered into the system, accepted for processing, and processed once and only once by the system and are properly included in output.
Component	A single resource with defined characteristics, such as a terminal or printer. These components are also defined by their relationship to other components.
Computer-assisted audit technique (CAAT)	Any automated audit technique, such as generalized audit software, test data generators, computerized audit programs, and special audit utilities.
Computer facility	A site or location with computer hardware where information processing is performed or where data from such sites are stored.

Exposure Draft

Computer operations	The function responsible for operating the computer and peripheral equipment, including providing the tape, disk, or paper resources as requested by the application systems.
Computer processing location	See computer facility.
Computer resource	See resource.
Computer room	Room within a facility that houses computers and/or telecommunication devices.
Computer security	Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated.
Computer system	A complete computer installation, including peripherals, in which all the components are designed to work with each other.
Computer-related controls	Computer-related controls help ensure the reliability, confidentiality, and availability of automated information. They include both general controls, which apply to all or a large segment of an entity's information systems, and application controls, which apply to individual applications.
Computing environment	Workstation or server (host) and its operating system, peripherals, and applications. .
Confidentiality	Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
Confidentiality control	Controls that are designed to provide reasonable assurance that application data and reports and other output are protected against unauthorized access.
Configuration auditing	Procedures for determining alignment between the actual system and the documentation describing it, thereby ensuring that the documentation used to support decision making is complete and correct.
Configuration control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.
Configuration control board	Evaluates and approves or disapproves proposed changes to configuration items and ensures implementation of approved changes
Configuration identification	Procedures for identifying, documenting, and assigning unique identifiers (for example, serial numbers and name) to a system's hardware and software component parts and subparts generally referred to as configuration items.
Configuration settings	Information system parameters that provide only essential capabilities and specifically prohibit or restrict the use of unnecessary functions, ports, protocols, and services.

Exposure Draft

Configuration status accounting	A procedure for documenting and reporting on the status of configuration items as a system evolves. Documentation, such as historical change lists and original designs or drawings, are generated and kept in a library, thereby allowing entities to continuously know the state of a system's configuration and be in a position to make informed decisions about changing the configuration.
Configuration management	The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system.
Console	Traditionally, a control unit such as a terminal through which a user communicates with a computer. In the mainframe environment, a console is the operator's station.
Contingency plan	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failure, or disaster.
Contingency planning	See contingency plan.
Continuity of Operations Plan (COOP)	A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.
Control activities	Descriptions of individual control requirements for each critical control element (e.g., implement effective authorization controls, adequately protect sensitive system resources).
Control categories	Groupings of related controls pertaining to similar types of risk. Control categories include security management, access controls, configuration management, segregation of duties, and contingency planning.
Control deficiency	In financial audits, a control deficiency in an entity's internal control over financial reporting exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.
Control deficiency	In single audits, a control deficiency in an entity's internal control over compliance exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect noncompliance with a type of compliance requirement of a federal program on a timely manner.
Control dependency	Exists when the effectiveness of an internal control is dependent on the effectiveness of other internal controls.

Exposure Draft

Control environment	The control environment is an important component of an entity's internal control structure. It sets the "tone at the top" and can influence the effectiveness of specific control techniques. Factors that influence the control environment include management's philosophy and operating style, the entity's organizational structure, methods of assigning authority and responsibility, management's control methods for monitoring and following up on performance, the effectiveness of the Inspector General's and internal audits, personnel policies and practices, and influences external to the entity.
Control objectives	The intent of the specific control to effectively secure specific general support or business activities.
Control risk	In a financial statement audit, the risk that a material misstatement that could occur in an assertion will not be prevented, or detected and corrected on a timely basis by the entity's internal control structure.
Control techniques	The specific control implemented by the entity to secure a specific general support system or business process activity.
Controlled Interface	Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
CPU	See central processing unit.
Critical control point	System control points that, if compromised, could allow an individual to gain unauthorized access to or perform unauthorized or inappropriate activities on entity systems or data, which could lead directly or indirectly to unauthorized access or modifications to the key areas of audit interest.
Cryptography	The science of coding messages so they cannot be read by any person other than the intended recipient. Ordinary text—or plain text—and other data are transformed into coded form by encryption and translated back to plain text or data by decryption.
Data	Facts and information that can be communicated and manipulated.
Data access method	See access method.
Data administration	The function that plans for and administers the data used throughout the entity. This function is concerned with identifying, cataloging, controlling, and coordinating the information needs of the entity.

Exposure Draft

Database	A collection of related information about a subject organized in a useful manner that provides a base or foundation for procedures, such as retrieving information, drawing conclusions, or making decisions. Any collection of information that serves these purposes qualifies as a database, even if the information is not stored on a computer.
Database administrator (DBA)	The individual responsible for both the design of the database, including the structure and contents, and the access capabilities of application programs and users to the database. Additional responsibilities include operation, performance, integrity, and security of the database.
Database management	Tasks related to creating, maintaining, organizing, and retrieving information from a database.
Database management system (DBMS)	(DB2, IMS, IDMS) A software product that aids in controlling and using the data needed by application programs. DBMSs organize data in a database, manage all requests for database actions—such as queries or updates from users—and permit centralized control of security and data integrity.
Data center	See computer facility.
Data communications	The transfer of information from one computer to another through a communications medium, such as telephone lines, microwave relay, satellite link, or physical cable.
Data communications systems	See data communications.
Data design	Organization of data into structures to facilitate retrieval while minimizing redundancy. The design of transaction data elements is a critical factor in helping assure the quality of data as well as its interrelationship with other data elements.
Data definition	Identification of all fields in the database, how they are formatted, how they are combined into different types of records, and how the record types are interrelated.
Data file	See file.
Data management systems	Applications which handle significant volumes of data often employ data management system to perform certain data processing functions within an application. Data management systems include database management systems, specialized data transport/communications software (often called middleware, cryptography used in conjunction with data integrity controls, data warehouse software and data reporting/data extraction software.
Data owner	See owner.
Data processing	The computerized preparation of documents and the flow of data contained in these documents through the major steps of recording, classifying, and summarizing.
Data processing center	See computer facility.

Exposure Draft

Data quality standard	Requirements to ensure the state of completeness, validity, consistency, timeliness and accuracy that makes data appropriate for a specific use.
Data security	See security management function.
Data strategy	Plan used to identify data needed to support business processes. A clearly defined data strategy minimizes data redundancies fundamental to an efficient, effective transaction processing function.
Data validation	Checking transaction data for any errors or omissions that can be detected by examining the data.
Data warehouse	A generic term for a system used to store, retrieve, and manage large amounts of data. A database, often remote, that contains recent snapshots of corporate data that can be used for analysis without slowing down day-to-day operations of the production database.
DBA	See database administrator.
DBMS	See database management system.
Debug	With software, to detect, locate, and correct logical or syntactical errors in a computer program.
Decryption	The process of changing ciphertext using a cryptographic algorithm and key.
Defense-in-depth	A commonly accepted "best practice" for implementing computer security controls in today's networked environments. Integrates people, operations, and technology capabilities to protect information systems across multiple layers.
Delete access	This level of access provides the ability to erase or remove data or programs.
Denial of Service (DOS)	The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)
Denial of Service (DOS) Attack	An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate
Detection risk	The risk that the auditor will not detect a material misstatement that exists in an assertion.
Dial-up access	A means of connecting to another computer, or a network similar to the Internet, over a telecommunications line using a modem-equipped computer.
Dial-back	Used as a control over dial-up telecommunications lines. The telecommunications link established through dial-up into the computer from a remote location is interrupted so the computer can dial back to the caller. The link is permitted only if the caller is from a valid phone number or telecommunications channel.

Exposure Draft

Digital Certificate	A certificate identifying a public key to its subscriber, corresponding to a private key held by that subscriber. It is a unique code that typically is used to allow the authenticity and integrity of communicated data to be verified.
Digital signature	Cryptographic process used to assure message originator authenticity, integrity, and nonrepudiation.
Direct access	An access method for finding an individual item on a storage device and accessing it directly, without having to access all preceding records.
Disaster recovery plan	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
Diskette	A removable and widely-used data storage medium that uses a magnetically coated flexible disk of Mylar enclosed in a plastic case.
DNS (domain name system)	A hierarchical database that is distributed across the Internet that allows names to be resolved into IP addresses (and vice versa) to locate services such as web and e-mail servers
DSS	See decision support system.
Download	Process of transferring data from a central computer to a personal computer or workstation.
Edit controls	Detects errors in the input portion of information that is sent to the computer for processing. The controls may be manual or automated and allow the user to edit data errors before processing.
Electronic signature	A symbol generated through electronic means that can be used to (1) identify the sender of information and (2) ensure the integrity of the critical information received from the sender. An electronic signature may represent either an individual or an entity. Adequate electronic signatures are (1) unique to the signer, (2) under the signer's sole control, (3) capable of being verified, and (4) linked to the data in such a manner that, if data are changed, the signature is invalidated upon verification. Traditional user identification code/password techniques do not meet these criteria.
Embedded Audit Module	Integral part of an application system that is designed to identify and report specific transactions or other information based on pre-determined criteria. Identification of reportable items occurs as part of real-time processing. Reporting may be real-time online, or may use store and forward methods. Also known as integrated test facility or continuous auditing module.
Encryption	Encryption is the conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized people.

Exposure Draft

Enterprise Resource Planning (ERP)	Commercial software that integrates all the information flowing through the entity. ERP systems contain functional modules (e.g., financial, accounting, human resources, supply chain, and customer information) that are integrated within the core system or interfaced to external systems.
Entity or component level	Controls at the entity or component level consist of the entitywide or componentwide processes designed to achieve the control activities. They are focused on how the entity or component manages IS related to each general control activity.
Entitywide information security program	An entitywide information security program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security management program establishes a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.
Entry points	Access points to the entity's information systems. This may include remote access through dial-up, wireless devices, or the Internet
Environmental controls	This subset of physical access controls prevents or mitigates damage to facilities and interruptions in service. Smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies are some examples of environmental controls.
Execute access	This level of access provides the ability to execute a program.
Exit	A predefined or in-house written routine that receives controls at a predefined point in processing. These routines provide an entity with the flexibility to customize processing, but also create the opportunity to bypass security controls.
Field	A location in a record in which a particular type of data are stored. In a database, the smallest unit of data that can be named. A string of fields is a concatenated field or record.
File	A collection of records stored in computerized form.
Financial management system	Financial information systems and the financial portions of mixed systems (systems that support both financial and nonfinancial functions) that are necessary to support financial management.
Firewall	Hardware and software components that protect one set of system resources (e.g., computers, networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users.
Firmware	Program recorded in permanent or semi permanent computer memory.

Exposure Draft

FISMA	Enacted into law as Title III of the E-Government Act of 2002 (PL 107-347; December 17, 2002), FISMA authorized and strengthened information security program, evaluation, and reporting requirements.
FMFIA	The objective of the Federal Managers' Financial Integrity Act of 1982 (FMFIA) is to provide reasonable assurance that (1) obligations and costs are in compliance with applicable law, (2) funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation, and (3) revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets.
Flowchart	A diagram of the movement of transactions, computer functions, media, and/or operations within a system. The processing flow is represented by arrows between symbolic shapes for operation, device, data file, etc. to depict the system or program.
Fraud	Fraud is a type of illegal act involving the obtaining of something of value through willful misrepresentation.
FTP (file transfer protocol)	A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.)
GAGAS	Also referred to as the Yellow Book. IT provides standards and guidance for use by government auditors to ensure that they maintain competence, integrity, objectivity, and independence in planning, conducting, and reporting their work, and are to be followed by auditors and audit organizations when required by law regulation, contract, agreement, or policy.
Gateway	In networks, a computer that connects two dissimilar local area networks, or connects a local area network to a wide area network, minicomputer, or mainframe. A gateway may perform network protocol conversion and bandwidth conversion.
General controls	General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. They include an entitywide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls.
General support system	An interconnected set of information resources under the same direct management control that shares common functionality. Normally, the purpose of a general support system is to provide processing or communications support.
Hacker	A person who attempts to enter a system without authorization from a remote location.
Hardware	The physical components of IT, including the computers, peripheral devices such as printers, disks, and scanners, and cables, switches, and other elements of the telecommunications infrastructure.

Exposure Draft

Hashing	Value computed on data to detect error or manipulation.
Hot site	A fully operational off-site data processing facility equipped with both hardware and system software to be used in the event of a disaster.
HTTP (hyper text transfer protocol)	A communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client browser.
HTTPS (hyper text transfer protocol secure)	A protocol for accessing a secure web server, whereby all data transferred is encrypted
Hub	A common connection point for devices in a network, hubs commonly is used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
Identification	The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.
IDS	See intrusion detection system.
IEEE	Institute of Electrical and Electronics Engineers)--Pronounced I-triple-E, IEEE is an organization composed of engineers, scientists and students. The IEEE is best known for developing standards for the computer and electronics industry.
Implementation	The process of making a system operational in the organization.
Incident	Assessed occurrence having actual or potentially adverse effects on an IS.
Incident response program	A process that involves detecting a problem, determining its cause, minimizing the damage it causes, resolving the problem, and documenting each step of the response for future reference.
Incompatible duties	When work responsibilities are not segregated so that one individual controls critical stages of a process incompatible duties exist.. For example, while users may authorize program changes, programmers should not be allowed to do so because they are not the owners of the system and do not have the responsibility to see that the system meets user needs. Similarly, one computer programmer should not be allowed to independently write, test, and approve program changes.
Information	The meaning of data. Data are facts; they become information when they are seen in context and convey meaning.
Information resource owner	See owner.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Exposure Draft

Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information system boundaries	Logical or physical boundaries around information resources and implementing measures to prevent unauthorized information exchange across the boundary in either direction. Firewall devices represent the most common boundary protection technology at the network level.
Information Security	Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provides integrity, confidentiality, and availability.
Information System (IS) Control	As defined in GAGAS, information system (IS) controls consist of those internal controls that are dependent on information systems processing and include general controls and application controls.
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information systems management	The function that directs or manages the activities and staff of the IS department and its various organizational components.
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, executive order, directive, policy, or regulation.
Infrastructure application	Include software that is used to assist in performing systems operations, including management of network devices. These applications include database, e-mail, browsers, plug-ins, utilities, and applications not directly related to business processes.
Input	Any information entered into a computer, or the process of entering data into the computer.
Integration testing	Testing to determine if related information system components perform to specifications.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. This involves ensuring that transmitted or stored data are not altered by unauthorized persons in a way that is not detectable by authorized users.
Interface	A connection between two devices, applications, or networks or a boundary across which two systems communicate. Interface may also refer to the portion of a program that interacts with the user.

Exposure Draft

Interface controls	Controls used to provide reasonable assurance that data used by applications that is input from legacy systems is reliable, valid, complete, and properly converted from the legacy application into the applications they support.
Interface design	Uses guidelines set by the strategy and provides specific information for each of the characteristics defined in the strategy. See Interface Strategy
Interface strategy	Describes at the highest level how the interfaces are implemented between two applications, The interface strategy includes an explanation of each interface, the interface method chosen (manual or batch, etc.), the data fields being interfaced, the controls to reasonably assure that the data is interfaced completely and accurately, timing requirements, assignment of responsibilities, on-going system balancing requirements, and security requirements.
Internal control	<p>(also referred to as internal control structure) A process, affected by agency management and other personnel, designed to provide reasonable assurance that (1) operations, including the use of agency resources, are effective and efficient; (2) financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use, are reliable; and (3) applicable laws and regulations are followed. Internal control also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition.</p> <p>Internal control consists of 5 interrelated components that form an integrated process that can react to changing circumstances and conditions within the agency. These components include the control environment, risk assessment, control activities, information and communication, and monitoring.</p>
Internet	When capitalized, the term "Internet" refers to the collection of networks and gateways that use the transmission control protocol/Internet protocol suite of protocols.
Internet protocol	Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.
Intrusion	Any intentional violation of the security policy of a system.
Intrusion Detection System (IDS)	An intrusion detection system (IDS) inspects network activity to identify suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system
Intranet	A private network that uses the infrastructure and standards of the Internet and World Wide Web, but is isolated from the public Internet by firewall barriers.

Exposure Draft

Inventory	FISMA requires that each agency develop, maintain, and annually update an inventory of major information systems operated by the agency or under its control. The inventory must include identification of the interfaces between agency systems and all other systems or networks, including interfaces not controlled by the agency.
Job	A set of data that completely defines a unit of work for a computer. A job usually includes programs, linkages, files, and instructions to the operating system.
Key	A long stream of seemingly random bits used with cryptographic algorithms. The keys must be known or guessed to forge a digital signature or decrypt an encrypted message.
Key area of audit interest	Those areas which are critical to achieving the audit objectives (e.g., general support and business process application systems and files or components thereof).
LAN	See local area network.
Label	See security label.
Least Privilege	Principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an IS.
Legacy system	A computer system consisting of older applications and hardware that was developed to solve a specific business problem. Many legacy systems do not conform to current standards, but are still in use because they solve the problem and replacing them would be too expensive.
Library	In computer terms, a library is a collection of similar files, such as data sets contained on tape and/or disks, stored together in a common area. Typical uses are to store a group of source programs or a group of load modules. In a library, each program is called a member. Libraries are also called partitioned data sets (PDS). Library can also be used to refer to the physical site where magnetic media, such as a magnetic tape, is stored. These sites are usually referred to as tape libraries.
Library control/ management	The function responsible for controlling program and data files that are either kept on-line or on tapes and disks that are loaded onto the computer as needed.
Library copier	Software that can copy source code from a library into a program.
Library management software	Software that provides an automated means of inventorying software, ensuring that differing versions are not accidentally misidentified, and maintaining a record of software changes.

Exposure Draft

Local area network (LAN)	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables a device to interact with any other on the network. Local area networks (LAN) commonly include microcomputers and shared (often expensive) resources such as laser printers and large hard disks. Most modern LANs can support a wide variety of computers and other devices. Separate LANs can be connected to form larger networks.
Log	With respect to computer systems, to record an event or transaction.
Log on	The process of establishing a connection with, or gaining access to, a computer system or peripheral device.
Logging file	See log.
Logical access control	The use of computer hardware and software to prevent or detect unauthorized access. For example, users may be required to input user identification numbers (ID), passwords, or other identifiers that are linked to predetermined access privileges.
Logical security	See logical access control.
Mainframe computer	A multi-user computer designed to meet the computing needs of a large organization. The term came to be used to refer generally to the large central computers developed in the late 1950s and 1960s to meet the accounting and information management needs of large organizations.
Maintenance	Altering programs after they have been in use for a while. Maintenance programming may be performed to add features, correct errors that were not discovered during testing, or update key variables (such as the inflation rate) that change over time.
Major application	OMB Circular A-130 defines a major application as an application that requires special attention due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification o, information in the application.
Malicious code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host.
Management controls	The organization, policies, and procedures used to provide reasonable assurance that (1) programs achieve their intended result, (2) resources are used that are consistent with the organization's mission, (3) programs and resources are protected from waste, fraud, and mismanagement, (4) laws and regulations are followed, and (5) reliable and timely information is obtained, maintained, reported, and used for decision making.

Exposure Draft

Master console	In MVS environments, the master console provides the principal means of communicating with the system. Other multiple console support (MCS) consoles often serve specialized functions, but can have master authority to enter all MVS commands.
Master data	Referential data that provides the basis for ongoing business activities, e.g., customers, vendors, and employees.
Master data controls	Controls over master data, the key information that is relatively constant and shared between multiple functions or applications (e.g., vendors, customers, employee's data, and vendor files).
Master data design	Layout of key data requirements to ensure integrity and utility of data information. Data integrity requirements include, for example, requiring an entry in all key fields, such as address and account number and not accepting invalid values in the required fields.
Master file	In a computer, the most currently accurate and authoritative permanent or semi-permanent computerized record of information maintained over an extended period.
Material weakness –A-123	A material weakness is a reportable condition in which the design or operation of the internal controls does not reduce to a relatively low level the risk that losses, noncompliance, or misstatements in amounts that would be material in relation to the principal statements or to a performance measure or aggregation of related performance measures may occur and not be detected within a timely period by employees in the normal course of their assigned duties.
Material weakness – A-123	Control deficiency or combination of control deficiencies that in management's judgement should be communicated because they represent significant weaknesses in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives.
Material weakness – financial reporting	A significant deficiency or combination of significant deficiencies that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.
Material weakness – single audit compliance	A significant deficiency or combination of significant deficiencies, that result in more than a remote likelihood that material noncompliance with a type of compliance requirement of a federal program will not be prevented or detected by the entity's internal control.
Materiality	An auditing concept regarding the relative importance of an amount or item. An item is considered not to be material when it is not significant enough to influence decisions or have an effect on the financial statements.

Exposure Draft

Media controls	Controls implemented to prevent unauthorized physical access to digital (e.g., diskettes, flash/thumb drives, compact disks) and printed media (e.g., paper, microfilm) removed from information system and during pick-up, transport, and delivery to authorized users.
Merge access	This level of access provides the ability to combine data from two separate sources.
Microcomputer	Any computer with its arithmetic logic unit and control unit contained in one integrated circuit, called a microprocessor.
Microprocessor	An integrated circuit device that contains the miniaturized circuitry to perform arithmetic, logic, and control operations (i.e. contains the entire CPU on a single chip).
Middleware	Another term for an application programmer interface (API). It refers to the interfaces that allow programmers to access lower- or higher-level services by providing an intermediary layer that includes function calls to the services.
Migration	A change from an older hardware platform, operating system, or software version to a newer one.
Mobile code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.
Mobile computing	Ability to use technology that is not physically connected, or in remote or mobile (non static) environments. Requires that the mobile computing activity be connected wirelessly to and through the internet or to and through a private network. This connection ties the mobile device to centrally located information and/or application software through the use of battery powered, portable, and wireless computing and communication devices. This includes devices like laptops with wireless LAN or wireless WAN technology, smart mobile phones, wearable computers and Personal Digital Assistants (PDAs).
Modem	Short for modulator-demodulator. A device that allows digital signals to be transmitted and received over analog telephone lines. This type of device makes it possible to link a digital computer to the analog telephone system. It also determines the speed at which information can be transmitted and received.
Multiyear testing plan	Where IS audits are performed on a regular basis the auditor may develop a multiyear audit plan. Such a plan will cover relevant key agency applications, systems, and processing centers. These strategic plans should cover no more than 3-year period and include the schedule and scope of assessments to be performed during the period and the rationale for planned approach.

Exposure Draft

Naming conventions	Standards for naming computer resources, such as data files, program libraries, individual programs, and applications.
Network	A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communications links. A network can be as small as a local area network consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area.
Network administration	The function responsible for maintaining secure and reliable network operations. This function serves as a liaison with user departments to resolve network needs and problems.
Network architecture	The underlying structure of a computer network, including hardware, functional layers, interfaces, and protocols (rules) used to establish communications and ensure the reliable transfer of information. Because a computer network is a mixture of hardware and software, network architectures are designed to provide both philosophical and physical standards for enabling computers and other devices to manage the complexities of establishing communications links and transferring information without conflict. Various network architectures exist, among them the internationally accepted seven-layer open systems interconnection model and International Business Machine (IBM) Systems Network Architecture. Both the open systems interconnection model and the Systems Network Architecture organize network functions in layers, each layer dedicated to a particular aspect of communication or transmission and each requiring protocols that define how functions are carried out. The ultimate objective of these and other network architectures is the creation of communications standards that will enable computers of many kinds to exchange information freely.
Network component	Devices that support a network including, workstations, servers, switches, and routers.
Network scanning	Procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment. Scanning procedures, such as ping sweeps and port scans, return information about which IP addresses map to live hosts that are active on the Internet and what services they offer. Another scanning method, inverse mapping, returns information about what IP addresses do not map to live hosts; this enables an attacker to make assumptions about viable addresses.
Network session	A connection between two network component peers. This provides the capability of bundling of resources needed for an instance of a service.

Exposure Draft

NIST	Under FISMA Act of 2002, the National Institute of Standards and Technology (NIST) develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support.
Node	In a local area network, a connection point that can create, receive, or repeat a message. Nodes include repeaters, file servers, and shared peripherals. In common usage, however, the term node is synonymous with workstation.
Nonrepudiation	The ability to prevent senders from denying that they have sent messages and receivers from denying that they have received messages.
Object code	The machine code generated by a source code language processor such as an assembler or compiler. A file of object code may be immediately executable or it may require linking with other object code files, e.g., libraries, to produce a complete executable program.
Object privilege	Allows the user to have access to the data within an object or allow the user to execute a stored program. These include: SELECT, INSERT, DELETE, etc. Each type of object has different privileges associated with it.
Off-the-shelf software	Software that is marketed as a commercial product, unlike custom programs that are privately developed for a specific client.
Online	A processing term that categorizes operations that are activated and ready for use. If a resource is online, it is capable of communicating with or being controlled by a computer. For example, a printer is online when it can be used for printing. An application is classified as online when users interact with the system as their information is being processed, as opposed to batch processing.
Online editors	See online program development software.
Online program development software	(TSO, ROSCOE, VOLLIE, ICCF, ISPF) Software that permits programs to be coded and compiled in an interactive mode.
Operating system	The software that controls the execution of other computer programs, schedules tasks, allocates storage, manages the interface to peripheral hardware, and presents a default interface to the user when no application program is running.
Operational controls	Relate to managing the entity's business and include policies and procedures to carry out organizational objectives, such as planning, productivity, programmatic, quality, economy, efficiency, and effectiveness objectives. Management uses these controls to provide reasonable assurance that the entity (1) meets its goals, (2) maintains quality standards, and (3) does what management directs it to do.

Exposure Draft

Output	Data/information produced by computer processing, such as graphic display on a terminal or hard copy.
Output devices	Peripheral equipment, such as a printer or tape drive, that provides the results of processing in a form that can be used outside the system.
Override	Decision made by agency management or operation staff to bypass established control(s) to allow a transaction or transactions that would otherwise be rejected by the system controls to be processed.
Owner	Manager or director who has responsibility for a computer resource, such as a data file or application program.
Packet	Data unit that is routed from source to destination in a packet-switched network. A packet contains both routing information and data. Transmission control protocol/Internet protocol (TCP/IP) is such a packet-switched network.
Packet Filtering	Controlling access to a network by analyzing the attributes of the incoming and outgoing packets and either letting them pass, or denying them, based on a list of rules
Parameter	A value that is given to a variable. Parameters provide a means of customizing programs.
Partitioning	Process of physically or logically separating different functions such as applications, security and communication activities. Separation may be accomplished by using different computers, different central processing units, different instances of the operating systems, different network addresses, or combinations of these methods.
Password	A confidential character string used to authenticate an identity or prevent unauthorized access.
Password Cracker	Specialized security checker that tests user's passwords, searching for passwords that are easy to guess by repeatedly trying words from specially crafted dictionaries. Failing that, many password crackers can brute force all possible combinations in a relatively short period of time with current desktop computer hardware.
Patch	Patches are additional pieces of code that have been developed to address specific problems or flaws in existing software. Vulnerabilities are flaws that can be exploited, enabling unauthorized access to IT systems or enabling users to have access to greater privileges than authorized.
Penetration testing	Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.
Peripheral	A hardware unit that is connected to and controlled by a computer, but that is external to the CPU. These devices provide input, output, or storage capabilities when used in conjunction with a computer.

Exposure Draft

Personally identifiable information	Refers to any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date of birth, or biometric records, and any other information which is linked or linkable to an individual.
Personnel controls	This type of control involves screening individuals prior to their authorization to access computer resources. Such screening should be commensurate with the risk and magnitude of the harm the individual could cause.
Personnel security	See personnel controls.
Physical access control	This type of control involves restricting physical access to computer resources and protecting these resources from intentional or unintentional loss or impairment.
Physical security	See physical access control.
Plain text	Data input to the Cipher or output from the Inverse Cipher.
Plans of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Platform	The foundation technology of a computer system. Typically, a specific combination of hardware and operating system.
Privacy Impact Assessment	An analysis of how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privileged account	Individuals who have access to set "access rights" for users on a given system. Sometimes referred to as system or network administrative accounts.
Privileged User	Individual who has access to system control, monitoring, or administration functions (e.g., system administrator, system security officer, maintainers, system programmers, etc.)
Process	Systematic sequences of operations to produce a specified result. This includes all functions performed within a computer such as editing, calculating, summarizing, categorizing, and updating.
Processing	The execution of program instructions by the computer's CPU.
Production control and scheduling	The function responsible for monitoring the information into, through, and as it leaves the computer operations area and for determining the succession of programs to be run on the computer. Often, an automated scheduling package is used in this task.

Exposure Draft

Production environment	The system environment where the agency performs its operational information processing activities.
Production programs	Programs that are being used and executed to support authorized organizational operations. Such programs are distinguished from “test” programs that are being developed or modified, but have not yet been authorized for use by management.
Profile	A set of rules that describe the nature and extent of access to available resources for a user or a group of users with similar duties, such as accounts payable clerks. (See standard profile and user profile.)
Program	A set of related instructions that, when followed and executed by a computer, perform operations or tasks. Application programs, user programs, system programs, source programs, and object programs are all software programs.
Program library	See library.
Programmer	A person who designs, codes, tests, debugs, and documents computer programs.
Proprietary	Privately owned, based on trade secrets, privately developed technology, or specifications that the owner refuses to divulge, which prevents others from duplicating a product or program unless an explicit license is purchased.
Protocol	In data communications and networking, a standard that specifies the format of data as well as the rules to be followed when performing specific functions, such as establishing a connection and exchanging data.
Public access controls	A subset of access controls that apply when an agency application promotes or permits public access. These controls protect the integrity of the application and public confidence in the application and include segregating the information made directly available to the public from official agency records.
Public domain software	Software that has been distributed with an explicit notification from the program’s author that the work has been released for unconditional use, including for-profit distribution or modification by any party under any circumstances.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Quality assurance	The function that reviews software project activities and tests software products throughout the software life cycle to determine if (1) the software project is adhering to its established plans, standards, and procedures and (2) the software meets the functional specifications defined by the user.
Query	The process of extracting data from a database and presenting it for use.

Exposure Draft

Read access	This level of access provides the ability to look at and copy data or a software program.
Real-time system	A computer and/or a software system that reacts to events before they become obsolete. This type of system is generally interactive and updates files as transactions are processed.
Record	A unit of related data fields. The group of data fields that can be accessed by a program and contains the complete set of information on a particular item.
Reliability	The capability of hardware or software to perform as the user expects and to do so consistently, without failures or erratic behavior.
Remote access	The process of communicating with a computer located in another place over a communications link.
Remote job entry (RJE)	With respect to computer systems with locations geographically separate from the main computer center, submitting batch processing jobs via a data communications link.
Remote Maintenance	Maintenance activities conducted by individuals communicating external to an information system security perimeter.
Reportable condition – A 123	Reportable conditions include matters coming to the auditor's attention that, in the auditor's judgment, should be communicated because they represent significant deficiencies in the design or operation of internal controls, which could adversely affect the entity's ability to meet its internal control objectives.
Repudiation	The denial by one of the parties to a transaction or participation in all or part of that transaction or of the content of communications related to that transaction.
Residual risk	Portion of risk remaining after security measures have been applied.
Resource	Something that is needed to support computer operations, including hardware, software, data, telecommunications services, computer supplies such as paper stock and preprinted forms, and other resources such as people, office facilities, and noncomputerized records.
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk analysis	The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.
Risk assessment	The identification and analysis of possible risks in meeting the agency's objectives that forms a basis for managing the risks identified and implementing deterrents.

Exposure Draft

Risk management	A management approach designed to reduce risks inherent in systems development and operations.
Router	An intermediary device on a communications network that expedites message delivery. As part of a LAN, a router receives transmitted messages and forwards them to their destination over the most efficient available route.
Run	A popular, idiomatic expression for program execution.
Run manual	A manual that provides application-specific operating instructions, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Sanitization	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
SAS 70	Statement on Auditing Standards No. 70: Service Organizations, commonly abbreviated as SAS 70, is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA), officially titled "Reports on the Processing of Transactions by Service Organizations". SAS 70 defines the professional standards used by a service auditor to assess the internal controls of a service organization and issue a service auditor's report. Service organizations are typically entities that provide outsourcing services that impact the control environment of their customers.
SDLC methodology	See system development life cycle methodology.
Security	The protection of computer facilities, computer systems, and data stored on computer systems or transmitted via computer networks from loss, misuse, or unauthorized access. Computer security, as defined by Appendix III to OMB Circular A-130, involves the use of management, personnel, operational, and technical controls to ensure that systems and applications operate effectively and provide confidentiality, integrity, and availability.
Security administrator	Person who is responsible for managing the security program for computer facilities, computer systems, and/or data that are stored on computer systems or transmitted via computer networks.
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

Exposure Draft

Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Label	Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.
Security management function	The function responsible for the development and administration of an entity's information security program. This includes assessing risks, implementing appropriate security policies and related controls, establishing a security awareness and education program for employees, and monitoring and evaluating policy and control effectiveness.
Security Objective	Confidentiality, integrity, or availability.
Security plan	A written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities and should outline the duties of those who are responsible for overseeing security (the security management function) as well as those who own, use, or rely on the entity's computer resources.
Security policy	The set of management statements that documents an organization's philosophy of protecting its computing and information assets. The set of security rules enforced by the system's security features
Security profile	See profile.
Security requirements	Requirements levied on an information system that are derived from laws, executive orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Security software	See access control software.
Segregation/separation of duties	A basic control that prevents or detects errors and irregularities by assigning responsibility for initiating transactions, recording transactions and custody of assets to separate individuals. Commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.

Exposure Draft

Sensitive information	Any information that an agency has determined requires heightened protection from unauthorized access, use, disclosure, disruption, modification, or destruction [e.g., by using specific access controls] because of the nature of the information (e.g., personal information required to be protected by the Privacy Act, proprietary commercial information, information critical to law enforcement activities, and information that has or may be determined to be exempt from public release under the Freedom of Information Act).
Sensitivity accounts	See privileged account
Server	A computer running administrative software that controls access to all or part of the network and its resources, such as disk drives or printers. A computer acting as a server makes resources available to computers acting as workstations on the network.
Service	Refers to customer or product-related business functions such as file transfer protocol (FTP), hypertext transfer protocol (HTTP), and mainframe supervisor calls. Each system provides a set of services. For example, a computer network allows its users to send packets to specified destinations and a database system responds to queries.
Service auditor	An independent auditor hired by the service organization to provide a report on internal controls at the service provider. See Service Organization.
Service Bureau	A computer facility that provides data processing services to clients on a continual basis
Service organization	Outside organizations used to support business processes. Service organizations provide services ranging from performing a specific task (e.g., payroll processing) to replacing entire business units or functions of an entity.
Significant deficiency – FISMA	A weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets.
Significant deficiency – A-123	OMB Circular A-123 uses the same definition for significant deficiency as financial reporting (See Significant Deficiency – Financial Reporting), but continues to refer to it as a reportable condition.
Significant Deficiency – financial reporting	A deficiency in internal control, or combination of deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected.

Exposure Draft

Significant deficiency – single audit compliance	A control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to administer a federal program such that there is more than a remote likelihood that noncompliance with a type of compliance requirement of a federal program that is more than inconsequential will not be prevented or detected by the entity's internal control.
Simultaneous peripheral operations online (SPOOL)	In the mainframe environment, a component of system software that controls the transfer of data between computer storage areas with different speed capabilities. Usually, an intermediate device, such as a buffer, exists between the transfer source and the destination (e.g., a printer).
Single audit	The single audit is intended to provide a cost-effective audit for nonfederal entities in that one audit is conducted in lieu of multiple audits of individual programs. Such audits are performed in accordance with the Single Audit Act of 1984 (with amendment in 1996) and OMB Circular A-133 (<i>Audits of States, Local Governments, and Non-Profit Organizations</i>) to ensure that federal funds to nonfederal entities are expended properly.
Smart card	A credit card-sized token that contains a microprocessor and memory circuits for authenticating a user of computer, banking, or transportation services.
SMTP (Simple Mail Transport Protocol)	The standard e-mail protocol on the Internet
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Social engineering	A method used by hackers to obtain passwords for unauthorized access. For example, a hacker may call an authorized user of a computer system and pose as a network administrator to gain access.
Software	A computer program or programs, in contrast to the physical environment on which programs run (hardware).
Source code	Human-readable program statements written in a high-level or assembly language, as opposed to object code, which is derived from source code and designed to be machine-readable.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge.
Standard	In computing, a set of detailed technical guidelines used as a means of establishing uniformity in an area of hardware or software development.
Standard profile	A set of rules that describe the nature and extent of access to each resource that is available to a group of users with similar duties, such as accounts payable clerks.

Exposure Draft

Supervisor call (SVC)	A supervisor call instruction interrupts a program being executed and passes control to the supervisor so that it can perform a specific service indicated by the instruction.
Switch	A device that forwards packets between LAN devices or segments. LANs that use switches are called switched LANs.
System	See information system.
System administrator	The person responsible for administering use of a multi-user computer system, communications system, or both.
System analyst	A person who designs systems.
System designer	See system analyst.
System developer	See programmer.
System development life cycle (SDLC) methodology	The policies and procedures that govern software development and modification as a software product goes through each phase of its life cycle.
System level	Controls consist of processes for managing specific system resources related to either a general support system or business process application systems. Three sublevels include network, operating system, and infrastructure.
System management facility	An IBM control program that provides the means for gathering and recording information that can be used to evaluate the extent of computer system usage.
System privilege	Ability of the user within the database to interact with the database itself. They include: CREATE, ALTER, DROP, CONNECT, and AUDIT, among many others.
System programmer	A person who develops and maintains system software.
System security plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
System software	The set of computer programs and related routines designed to operate and control the processing activities of computer equipment. It includes the operating system and utility programs and is distinguished from application software.
System testing	Testing to determine that the results generated by the enterprise's information systems and their components are accurate and the systems perform to specifications.
System utilities	Software used to perform system maintenance routines that are frequently required during normal processing operations. Some of the utilities have powerful features that will allow a user to access and view or modify data or program code.
TCP (transmission control protocol)	A connection-based Internet protocol that supports reliable data transfer connections. Packet data is verified using checksums and retransmitted if it is missing or corrupted. The application plays no part in validating the transfer.

Exposure Draft

TCP/IP protocol	Transmission Control Protocol/Internet Protocol) A set of communications protocols that encompasses media access, packet transport, session communications, file transfer, electronic mail, terminal emulation, remote file access and network management. TCP/IP provides the basis for the Internet.
Technical controls	See logical access control.
Telecommunications	A general term for the electronic transmission of information of any type, such as data, television pictures, sound, or facsimiles, over any medium, such as telephone lines, microwave relay, satellite link, or physical cable.
Teleprocessing monitor	In the mainframe environment, a component of the operating system that provides support for online terminal access to application programs. This type of software can be used to restrict access to online applications and may provide an interface to security software to restrict access to certain functions within the application.
Terminal	A device consisting of a video adapter, a monitor, and a keyboard.
Test facility	A processing environment that is isolated from the production environment and dedicated to testing and validating systems and/or their components.
Those charged with governance	Are those responsible for overseeing the strategic direction of the entity and the entity's fulfillment of its obligations related to accountability. This includes overseeing the financial reporting process, subject matter, or program under audit including related internal controls.
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Token	In authentication systems, some type of physical device (such as a card with a magnetic strip or a smart card) that must be in the individual's possession in order to gain access. The token itself is not sufficient; the user must also be able to supply something memorized, such as a personal identification number (PIN).
Transaction	A discrete activity captured by a computer system, such as the entry of a customer order or an update of an inventory item. In financial systems, a transaction generally represents a business event that can be measured in money and entered in accounting records.
Transaction data	The finite data pertaining to a given event occurring in a business process. The result of this process is in the form of documents or postings, such as purchase orders and obligations.

Exposure Draft

Transaction data input	Relates to controls over data that enter the application (e.g., data validation and edit checks).
Transaction data output	Relates to controls over data output and distribution (e.g., output reconciliation and review).
Transaction data processing	Relates to controls over data integrity within the application (e.g., review of transaction processing logs).
Transaction file	A group of one or more computerized records containing current business activity and processed with an associated master file. Transaction files are sometimes accumulated during the day and processed in batch production overnight or during off-peak processing periods.
Trusted communication Path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.
Uninterruptible power supply (UPS)	Provides short-term backup power from batteries for a computer system when the electrical power fails or drops to an unacceptable voltage level
Unit testing	Testing individual program modules to determine if they perform to specifications.
UNIX	A multitasking operating system originally designed for scientific purposes that have subsequently become a standard for midrange computer systems with the traditional terminal/host architecture. UNIX is also a major server operating system in the client/server environment.
Update access	This access level includes the ability to change data or a software program.
Upload	The process of transferring a copy of a file from a local computer to a remote computer by means of a modem or network.
User	The person who uses a computer system and its application programs to perform tasks.
User auditor	The auditor of the user organization.
User control	Portions of controls that are performed by people interacting with IS controls. The effectiveness of user controls typically depend on the accuracy of the information produced by the IS controls.
User-defined processing	The user is allowed to establish or modify processing steps. This frequently occurs in application based spreadsheets and report writer/data extraction tools.
User identification (ID)	A unique identifier assigned to each authorized computer user.
User privilege	Right to execute a particular type of Microsoft SQL server statement, or a right to access another user's object

Exposure Draft

User profile	A set of rules that describes the nature and extent of access to each resource that is available to each user.
Utility program	Generally considered to be system software designed to perform a particular function (e.g., an editor or debugger) or system maintenance (e.g., file backup and recovery).
Validation	The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.
Validity	See Validity Control.
Validity Control	Controls designed to provide reasonable assurance (1) that all recorded transactions actually occurred (are real), relate to the entity, and were properly approved in accordance with management's authorization, and (2) that output contains only valid data.
Virtual Private Network (VPN)	Protected IS link utilizing tunneling, security controls (see information assurance), and end-point address translation giving the impression of a dedicated line.
Virus	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in an information system.
Vulnerability scanning	Type of network security testing that among others enumerates the network structure and determines the set of active hosts and associated software and verifies that software (e.g., operating system and major applications) is up-to-date with security patches and software version.
Wide area network (WAN)	A group of computers and other devices dispersed over a wide geographical area that is connected by communications links.
WAN	See wide area network.
War Dialer	Software packages that sequentially dial telephone numbers, recording any numbers that answer.
Web application	Is an application that is accessed via web over a network such as the Internet or an intranet. The ability to update and maintain Web applications without distributing and installing software on potentially thousands of client computers is a key reason for their popularity.

Exposure Draft

Wired Equivalent Privacy (WEP)	The Wired Equivalent Privacy (WEP) security protocol for wireless local area networks (LANs) uses encryption to provide similar security to that of a wired LAN. WEP is defined in the IEEE 802.11b standard.
Wi-Fi Protected Access (WPA)	The Wi-Fi Protected Access (WPA) security protocol was designed to improve upon the security features of WEP for wireless communications. It is defined in IEEE's 802.11i standard.
Workstation	A microcomputer or terminal connected to a network. Workstation can also refer to a powerful, stand-alone computer that has considerable calculating or graphics capability.
World Wide Web (WWW)	A sub-network of the Internet through which information is exchanged by text, graphics, audio and video.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.

Exposure Draft

Appendix XIII – Bibliography

Committee on National Security Systems, *National Information Assurance (IA) Glossary*, CNSS Instruction No. 4009 (Ft Meade, Maryland: Revised Draft 2005).

Information System Audit and Control Association (ISACA), *Glossary of Terms*, <http://www.isaca.org/glossary.htm>.

Office of Management and Budget, *Security of Federal Automated Resources*, Circular A-130, Appendix III, (Washington, D.C.: November 2000).

Office of Management and Budget, *Management Responsibility for Internal Control*, Circular A-123, Appendix A, (Washington, D.C.: July 2005).

Office of Management and Budget, *Designation of Senior Agency Officials for Privacy*, Memorandum M-05-08 (Washington, D.C.: February 11, 2005).

Office of Management and Budget, *Safeguarding Personally Identifiable Information*, Memorandum M-0615 (Washington, D.C.: May 22, 2006).

Office of Management and Budget, *Protection of Sensitive Agency Information*, Memorandum M-06-16 (Washington, D.C.: June 23, 2006).

Office of Management and Budget, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, Memorandum M-06-19 (Washington, D.C.: July 12, 2006).

Office of Management and Budget, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Memorandum M-06-20 (Washington, D.C.: July 17, 2006).

Exposure Draft

Office of Management and Budget, *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements*, Memorandum M-07-04 (Washington, D.C.: December 22, 2006).

Office of Management and Budget, *Implementation of Commonly Accepted Security Configurations for Window Operating Systems*, (Washington, D.C.: March 22, 2007).

Office of Management and Budget, *Safeguarding Against and Responding to the Breach of Personally identifiable Information*, Memorandum M-07-16 (Washington, D.C.: May 22, 2007).

U.S. Department of Commerce, National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards 140-2, (Washington, D.C.: May 2001).

U.S. Department of Commerce, National Institute of Standards and Technology, *Advance Encryption Standard (AES)*, Federal Information Processing Standards 197, (Washington, D.C.: November 2001).

U.S. Department of Commerce, National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards 199, (Washington, D.C.: February 2004).

U.S. Department of Commerce, National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards 200, (Washington, D.C.: March 2006).

U.S. Department of Commerce, National Institute of Standards and Technology, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, Federal Information Processing Standards 201, (Washington, D.C.: March 2006).

U.S. Department of Commerce, National Institute of Standards and Technology, *Glossary of Key Information Security Terms*, (Washington, D.C.: April 2006).

Exposure Draft

U.S. Department of Commerce, National Institute of Standards and Technology, *Introduction to Computer Security*, Special Publication 800-12, (Washington, D.C.: October 1995).

U.S. Department of Commerce, National Institute of Standards and Technology, *Information Technology Security Training Requirements: A Role-Performance-Based Model*, Special Publication 800-16, (Washington, D.C.: April 1998).

U.S. Department of Commerce, National Institute of Standards and Technology, *Guide for Developing Security Plans for Federal Information Systems*, Special Publication 800-18, (Washington, D.C.: February 2006).

U.S. Department of Commerce, National Institute of Standards and Technology, *Guideline for Implementing Cryptography in the Federal Government*, Special Publication 800-21, (Washington, D.C.): December 2005).

U.S. Department of Commerce, National Institute of Standards and Technology, *Engineering Principles for Information Technology Security*, Special Publication 800-27, (Washington, D.C.: June 2004).

U.S. Department of Commerce, National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems*, Special Publication 800-30, (Washington, D.C.: July 2002).

U.S. Department of Commerce, National Institute of Standards and Technology, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, Special Publication 800-32, (Washington D.C.: February 2001).

U.S. Department of Commerce, National Institute of Standards and Technology, *Contingency Planning Guide for Information Technology Systems*, Special Publication 800-34, (Washington, D.C.: June 2002).

U.S. Department of Commerce, National Institute of Standards and Technology, *Guide to Information Technology Security Services*, Special Publication 800-35, (Washington, D.C.: October 2003).

Exposure Draft

U.S. Department of Commerce, National Institute of Standards and Technology, *Guide for Security Certification and Accreditation of Federal Information Systems*, Special Publication 800-37, (Washington, D.C.: May 2004).

U.S. Department of Commerce, National Institute of Standards and Technology, *Creating a Patch and Vulnerability Management Program*, Special Publication 800-40, (Washington, D.C.: November 2005).

U.S. Department of Commerce, National Institute of Standards and Technology, *Guideline on Network Security*, Special Publication 800-42, (Washington, D.C.: November 2002).

U.S. Department of Commerce, National Institute of Standards and Technology, *Security for Telecommuting and Broadband Communications*, Special Publication 800-46, (Washington, D.C.: August 2002).

U.S. Department of Commerce, National Institute of Standards and Technology, *Security Guide for Interconnecting Information Technology Systems*, Special Publication 800-47, (Washington, D.C.: August 2002).

U.S. Department of Commerce, National Institute of Standards and Technology, *Building an Information Technology Security Awareness and Training Program*, Special Publication 800-50, (Washington, D.C.: October 2003).

U.S. Department of Commerce, National Institute of Standards and Technology, *Recommended Security Controls for Federal Information*, Special Publication 800-53. (Washington, D.C.: February 2005).

U.S. Department of Commerce, National Institute of Standards and Technology, *Security Metrics Guide for Information Technology Systems*, Special Publication 800-55, (Washington, D.C.: July 2003).

U.S. Department of Commerce, National Institute of Standards and Technology, *Recommendation for Pair-Wise Key Establishment*

Exposure Draft

Schemes Using Discrete Logarithm Cryptography, Special Publication 800-56, (Washington, D.C.: March 2006).

U.S. Department of Commerce, National Institute of Standards and Technology, *Security Considerations for Voice over IP Systems*, Special Publication 800-58, (Washington, D.C.: January 2005).

U.S. Department of Commerce, National Institute of Standards and Technology, *Recommendation for Key Management*, Special Publication 800-57, (Washington, D.C.: August 2005).

U.S. Department of Commerce, National Institute of Standards and Technology, *Guide for Mapping Types of Information and Information System Security Categories*, Special Publication 800-60, (Washington, D.C.: June 2004).

U.S. Department of Commerce, National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61, (Washington, D.C.: January 2004).

U.S. Department of Commerce, National Institute of Standards and Technology, *Electronic Authentication Guidelines*, Special Publication 800-63, (Washington, D.C.: April 2006).

U.S. Department of Commerce, National Institute of Standards and Technology, *Security Considerations in the Information System Development Life Cycle*, Special Publication 800-64, (Washington, D.C.: June 2004).

U.S. Department of Commerce, National Institute of Standards and Technology, *Security Configuration Checklists Program for IT Products*, Special Publication 800-70, (Washington, D.C.: May 2005).

U.S. Department of Commerce, National Institute of Standards and Technology, *Interfaces for Personal Identity Verification*, Special Publication 800-73, (Washington, D.C.: March 2006).

U.S. Department of Commerce, National Institute of Standards and Technology, *Biometric Data Specifications for Personal Identity Verification*, Special Publication 800-76, (Washington, D.C.: January 2007).

Exposure Draft

U.S. Department of Commerce, National Institute of Standards and Technology, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, Special Publication 800-78, (Washington, D.C.: August 2007).

U.S. Department of Commerce, National Institute of Standards and Technology, *Guide to Intrusion Detection and Prevention Systems*, Special Publication 800-94, (Washington, D.C.: February 2007).

U.S. Department of Commerce, National Institute of Standards and Technology, *Establishing Wireless Robust Security Networks*, Special Publication 800-97, (Washington, D.C.: February 2007).

U.S. Department of Commerce, National Institute of Standards and Technology, *Information Security Handbook: A Guide for Managers*, Special Publication 800-100, (Washington, D.C.: March 2007).

U.S. Department of Justice, *Vulnerability Assessment of Federal Facilities*, (Washington, D.C.: June 28, 1995).

U.S. General Accounting Office, *Executive Guide: Information Security Management, Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

U.S. General Accounting Office, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-01.3.1 (Washington, D.C.: November 1999).

U.S. General Accounting Office, *Key Elements of a Risk Management Approach*, GAO-02-150T (Washington, D.C.: October 2001).

U.S. General Accounting Office, *Technologies to Secure Federal Buildings*, GAO-02-687T (Washington, D.C.: April 2002).

U.S. General Accounting Office, *Assessing the Reliability of Computer-Processed Data*, (Washington, D.C. October 2002).

Exposure Draft

U.S. Government Accountability Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6. (Washington, D.C.: January 1999).

U.S. Government Accountability Office, *Government Auditing Standards*, GAO-07-162G (Washington, D.C.: July 2007).