United States General Accounting Office

159362

GAO

Accounting and Information Management Division

May 1997

The System Assessment Framework, Version 1.1

A Guide for Reviewing Information Management and Technology Issues in the Federal Government

GAO/AIMD-10.1.12

Preface

Today, the vast majority of government's day-to-day operations are run electronically using complex information and communications systems linking hundreds and often thousands of mainframe and personal computers. The Office of Management and Budget (OMB) estimates that by the year 2000, 75 percent of all public transactions will be handled electronically. Clearly, information management has become a critical factor in achieving efficient and quality government operations for Americans.

Developing and maintaining this capability through effective and efficient information systems has been a challenging process. In excess of $25 billion annually is spent by agencies developing and/or maintaining information systems to improve critical operations. More often than not, the process is thwarted by excessive cost overruns and schedule delays, or a system is developed that does not meet an agency's objectives and strategic information needs. Typical causes for these problems involve requirements that are not adequately defined, inadequate user participation in the development process, or inadequate system testing.

The responsibilities inherent in developing major mission critical information systems that has apply to federal agencies also have a significant impact on the government's audit capability. Because of the pervasiveness of information systems to government operations and the effect of these systems the on integrity and reliability of information, government audit organizations are becoming increasingly concerned with developing a systems auditing capability to evaluate critical information systems development and maintenance issues. No longer can federal audit organizations rely solely on accounting standards to form opinions on agency operations, because a detailed understanding of the information necessary for agencies to meet their missions and the automated systems they use has now become a prerequisite.

The General Accounting Office (GAO), in fulfilling its increasing responsibilities for evaluating critical government operations is improving its capability to evaluate automated systems, including the resources and procedures needed to manage them. To facilitate this development, GAO has developed the System Assessment Framework (SAF), a standardized methodology for evaluating critical issues associated with automated systems development and operations. The methodology was based on principles and practices for evaluating automated information systems from Arthur Anderson's Method One, International Standards Organization's (ISO) 9000 series of standards, the Software Engineering Institute's Capability Maturity Model, the Department of Defense's Automated Information System Life Cycle Management Policy, and other private and public sector methodologies. Use of this standardized approach will enable GAO to satisfy the following needs.

First, GAO evaluators must be aware of the importance of automated information systems life-cycle issues. In today's technology-dependent program environment, few federal programs can be evaluated effectively without considering the economy, effectiveness, and efficiency of information system development life-cycle issues.

Second, GAO must use a consistent and disciplined approach for conducting automated information system life-cycle (AISLC) reviews. GAO's methodology draws upon its collective information systems audit experience and provides a useful, disciplined, and consistent approach for identifying key issues and developing audit programs to address them.

Third, a common language is needed for executing AISLC-related reviews. Establishing a common language is important for facilitating communication and working relationships among auditors, evaluators, and specialists of diverse backgrounds. It is also useful for developing training courses.

The methodology is primarily intended for GAO's information systems analysts and evaluators to use as a tool when performing reviews of individual system development projects. It may also be useful for program managers, Inspector General (IG) offices, and external auditors in their program acquisition and oversight activities. The methodology provides criteria and a process that agencies can follow when planning, acquiring, and operating automated systems and some general audit steps to help the evaluator prepare an audit or evaluation plan. It is important, however, to recognize that the methodology is not a prescriptive cookbook that tells the evaluator what to do in every AISLC audit. Rather, it satisfies GAO's need for a generalized, procedural framework that is flexible enough to allow deeper technical scrutiny when warranted. The methodology is not intended to be used in its entirety for every audit assignment. Rather, segments applicable to the scope of the assignment should be selected.

The methodology was prepared under the direction of William S. Franklin, Director, Information Systems Methodology and Support, who can be reached at (202) 512-6408.

Gene L. Dodaro
Assistant Comptroller General
Accounting and Information Management Division

Major Contributors to this Publication

Accounting and Information Management Division, Washington, D.C.

William S. Franklin, Director
Frank W. Reilly, Director
Prithviraj Mukherji, Assistant Director
Paul Silverman, Project Manager
David Chao, Principal Architect
Martin E. Caulk, Information Systems Analyst
Gary R. Austin, Senior Technical Advisor

Acknowledgments

We would like to express our sincere and deep appreciation to the individuals that originally started this effort at GAO, Donald Chapin (Chief Accountant), Richard C. Lavelle (Director), Barry Kauffman (Director), Vincent DeSanti (Assistant Director), Leonard J. Latham (Assistant Director) and Danny Latta (Assistant Director). Additionally, we offer a special thank you to Rona Stillman (Chief Scientist) for an excellent in-depth review of this methodology. Rose Hernandez, Madhav Panwar, Ernie Stockel, Alan Merrill, Keith Rhodes, Michael Fruitman and Janet Eackloff provided constructive critique as SAF progressed from exposure draft to version 1.0. Finally, we wish to express our gratitude to Ira Sachs, Eugene Kudla, John Riley, and Tonia Johnson for their assistance. The diligent efforts of these individuals, and reviews by other GAO staff are largely responsible for the quality and uniformity we have attempted to achieve in this document.

Table of Contents

Design, Development, and Deployment

Operations and Maintenance

Abbreviations

ADP	Automated Data Processing
AIS	Automated Information System
AISLC	Automated Information System Life-Cycle
APR	Agency Procurement Request
CAD	Computer Aided Design
CASE	Computer Aided Software Engineering
COCOMO	Constructive Cost Model
COTS	Commercial Off the Shelf Software
DOD	Department of Defense
DPA	Delegation of Procurement Authority
GAO	General Accounting Office
GMR	General Management Review
GSA	General Services Administration
IG	Inspector General
IOC	Initial Operating Capability
IRM	Information Resources Management
ISO	International Standards Organization
IV&V	Independent Verification and Validation
OMB	Office of Management and Budget
PERT	Project Evaluation and Review Technique
QA	Quality Assurance
RFP	Request for Proposal
ROC	Required Operating Capability
SAF	System Assessment Framework
SCE	Software Capability Evaluation
SLIM	Software Life Cycle Management Model

Overview

Effective use of computer-based information systems is crucial to both the delivery and the quality of products and services For executives and program managers, timely, relevant, and accurate information is essential for measuring and depicting the status, inputs, outcomes, and success of program operations. Most federal managers depend on information systems to process, safeguard, access, and disseminate information to support program oversight and executive decision-making. The ability to achieve effective management and operations of key information systems should be a top management priority.

GAO evaluation teams should use the System Assessment Framework (SAF) as a tool to facilitate an evaluation of the major systems and modernization initiatives of federal agencies. SAF is a generic representation of generally accepted principles of systems planning, analysis, design, development, deployment, operations, and maintenance. Using SAF, evaluation teams should be able to quickly identify key risk factors in agency developmental initiatives and operations. This overview provides general guidance on how the team should use the methodology to help achieve this goal.

The System Assessment Framework

Government and industry have developed methodologies for guiding an agency through the many activities that must be performed in planning and developing information systems to meet its needs. The General Services Administration (GSA) has identified over 20 methodologies that have been developed by government agencies for their use. Although the methodologies may use different terminologies, they all subscribe to a generally accepted sequence of events called life-cycle phases. GAO's methodology draws heavily on the generally accepted sequence of events described in these methodologies. Therefore, SAF is a meta-model from which many existing instances of system development methodologies can be derived. The specific instances of methodologies differ only in that they emphasize different facets of system life-cycle concepts because of their unique requirements. SAF emphasizes the importance of linking the agency's business mission, programmatic strategic objectives, operational characteristics, and the Information Resources Management (IRM) strategic planning process to its system design, development, and operational activities.

SAF Life Cycle Phases

The SAF methodology has been developed around a four phase automated information system life cycle (AISLC) which includes generally accepted principles of systems planning, analysis, design, development, deployment, operations, and maintenance. Phase I discusses how the agency's strategic IRM and program planning processes ties into its system design, development, and operational activities. This includes identifying the agency's mission, needs,

and objectives; evaluating how the agency's current operations are being met (i.e., organizational responsibilities, planning, policies and standards, and quality assurance and internal audit functions); defining the agency's strategic direction for automating the program function under review; and estimating the resources necessary to accomplish the AISLC development activities. Phases 2 through 4 describe the concept and project initiation; system design, development, and deployment; and operations and maintenance phases within the automated information system (AIS) life cycle. The following provides more specific detail on each phase.

Planning Phase

Information planning is a periodic, structured process that establishes a corporate-level, strategic view of how information systems affecting program operations will be changed and/or acquired and used to support the agency over a 3 to 5 year period. From this process, an audit team will be able to use SAF to evaluate how the system under development fits into the agency's overall strategic information plan.

Activities in the planning phase are usually the responsibility of a senior-level official. These activities include establishing agency-wide IRM goals, providing top-down guidance on policy and program goals, reviewing and approving component plans, which are developed from the bottom up, and assisting subagency managers to obtain budget approval for system acquisitions. During this phase, the agency is primarily concerned with determining a strategy and preparing an action plan to change the current IRM environment so that it will better support current activities as well as new and emerging priorities.

In order to generate plans linked to real world operational conditions (including deficiencies), planners must obtain feedback from analyses of the existing method of operations, business area analysis and design, and the organization's culture or philosophy. Planners must take into consideration impediments to moving the organization from its existing method of operations to a modified and improved method of operations.

Concept Phase

After the agency has completed its information planning process it is ready to begin developing the high-priority system development projects identified in its action plan. The concept and project initiation phase consists of planning and organizing tasks for the project. Additionally, this phase continues to refine the business area analysis so as to be able to develop the concept of operations. This is different from IRM planning, which identifies and/or defines the agencywide high-level requirements and service-level objectives, as well as the short- and long-term automation objectives of the agency. During the concept phase, the agency organizes and approves a specific system development project, and its requirements are detailed to the level that permits a system design to be created in the next phase.

System Design, Development, and Deployment Phase

Following concept approval, an agency enters the system design, development, and deployment phase. There are two distinct approaches that can be taken, (1) iterative design, development, and deployment or (2) custom design, development, and deployment. A third option exists, which is known as the purchase of a commercial-off-the-shelf (COTS) product, but usually such a product must be integrated, customized, or both to be incorporated into a large complex AIS. Given this fact, COTS are addressed in the context of either the iterative or custom approaches. On a major AIS, it is not unusual to see a combination of these approaches in use. Therefore, the evaluation team needs to quickly gain insight into the scope of the effort being attempted by the agency to decide if the development approach taken by the agency is prudent given the size, complexity, and risk associated with the initiative. SAF is designed to provide guidance on multiple system design and development approaches that may be used on an agency automation initiative.

System Operation and Maintenance Phase

In the operations and maintenance phase, appropriate organizational units within the agency take ownership and responsibility for operating and maintaining the system that evolved through the previous planning, concept and project initiation, and design, development, and deployment phases. This phase is thus concerned with ensuring a stable and secure day-to-day operating environment, adequate system performance (e.g., responsiveness or reliability), user satisfaction (e.g., ease of use or availability), continuity of operations (including disaster recovery), a comprehensive hardware and software configuration control process, and a controlled problem-management process (i.e., usually a combination of preventive and remedial maintenance). System operations must be performed in a controlled environment in accordance with the agency's policies, standards, and procedures, as well as conform to operating plans, budgets, and legal and regulatory requirements.

During this phase, users frequently change their functional and operational requirements until the volume and rate of change becomes so extensive that a new program or major modernization initiative is required.

Organization of the SAF Methodology

SAF is organized around the four phase systems life-cycle approach described above. Each phase begins by graphically portraying the components of the phase. The use of these diagrams allow easy identification of the parts of the phase required by the assignment, as well as the applicable segments within each part. Each segment section lists activities that the agency should be taking, audit objectives, commonly expected documentation, and audit tasks.

The appendix contain tools that play an integral role in successfully applying the SAF methodology. They include references for developing agency and system profiles as essential background information for performing an AISLC audit, applicable criteria related to AISLC life-cycle phases, list of related methodologies, a quick reference guide, and worksheets for documenting audit activities performed and for summarizing audit findings.

In using the appendix, particular attention should be placed on appendix A. This appendix contains guidelines for preparing an agency and systems profile, which are useful tools in obtaining pertinent background information for planning or performing any audit work using SAF. The agency profile contains information about the agency unit, program, or activity under review. It includes the following information: mission, goals and objectives of the unit, status of the unit's IRM environment; organization, standards, policies, and procedures; critical information flows and the resources to support them; the key information providers, handlers, and users; and related studies, audits, and reviews. The system profile contains information on the hardware architecture and configurations, software (i.e., system software such as MVS/XA, support software such as compilers, utilities, and application software), communications and information architecture.

Guidelines for Usage

SAF should be used throughout the audit to provide guidance and criteria for system development auditing activities. In the early stages of an audit, SAF should be used as guidance in the preparation of the audit plan, design matrix, and in the staffing of the multidisciplinary audit team.

SAF provides guidance on "what to do" in evaluating automated information systems but leaves the "how to" up to experienced team members in the various occupational disciplines. As such, it is not a cookbook. Teams are expected to be formed in full adherence to chapter 3 of GAO's "Government Auditing Standards: 1994 Revision (GAO/OCG-94-4)," dated June 1994.

SAF emphasizes the strong link that must exist between an agency's business operations and the information systems or computer-based systems that support this mission. It is applicable across the broad spectrum of activities within the system's life cycle. The methodology recognizes the constraints on the federal budgetary, cultural, and service environment in which federal agencies operate. SAF was designed for evaluating information management and technology issues in the federal government. It emphasizes the use of multidisciplinary teams consisting of program analysts, business process analysts, information systems analysts, and ADP/telecommunication analysts. Team participants should have completed the SAF training course, "Overview of the System Assessment Framework" prior to using SAF.

Contents of the Planning Phase

1.0 The Planning Phase

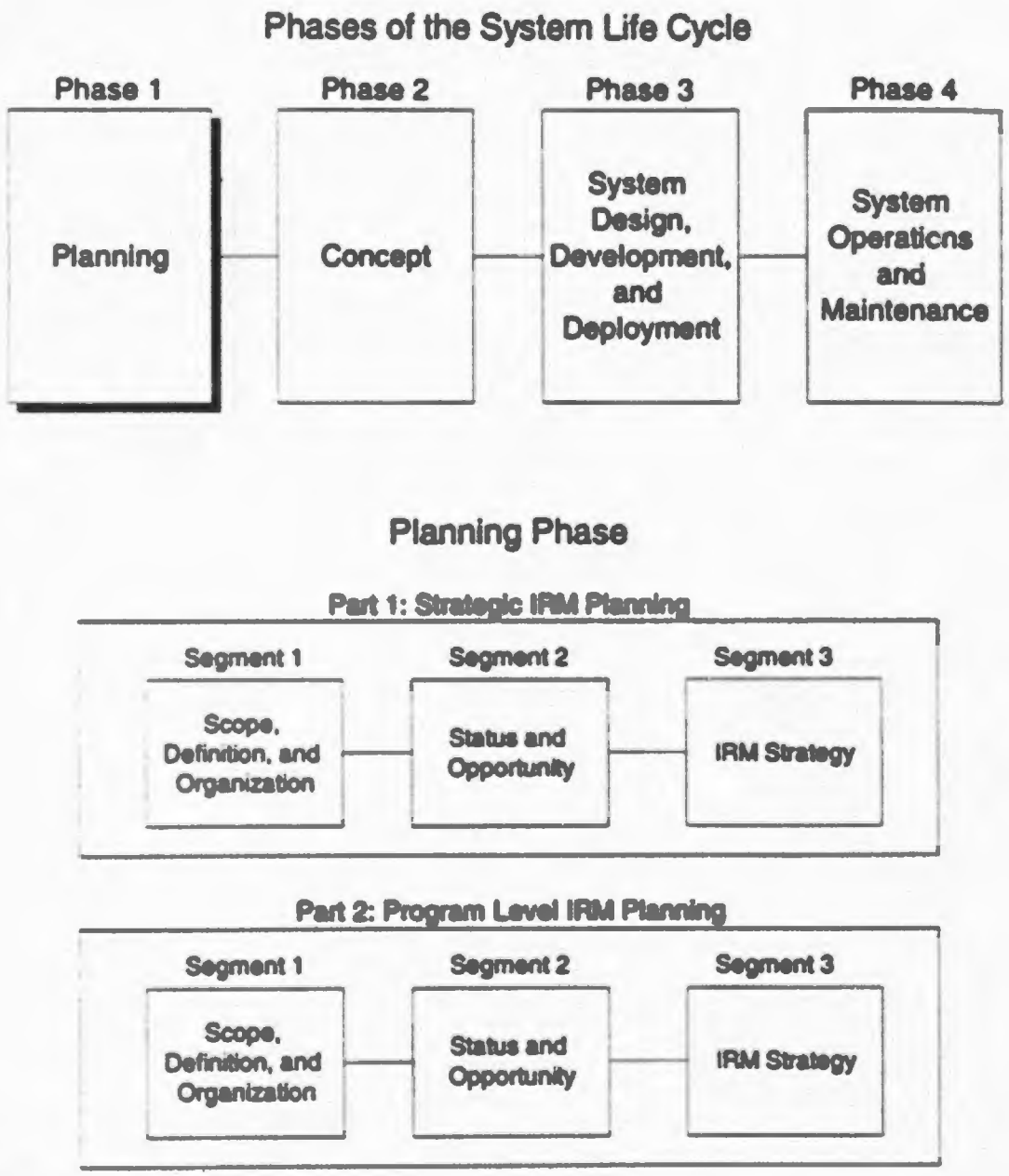

Figure 1. The Planning Phase

The way an agency manages its information resources[1] can make a vital difference between success or failure in accomplishing program objectives. Information should be considered as a fourth business resource which is in addition to capital, human resources, and plant and equipment (facilities) because it has value, costs money (to collect, process, and disseminate), has qualities affecting program outcomes (accuracy, and timeliness), and can be controlled (accounted for and managed). The availability of government information in diverse media, including electronic formats, permits greater flexibility in its use. Information technology is only a means for transforming information from one medium into another; it is not an end in itself. When used judiciously in conjunction with redesigning work processes, information technology presents opportunities to improve the effectiveness and efficiency of program operations and service delivery.

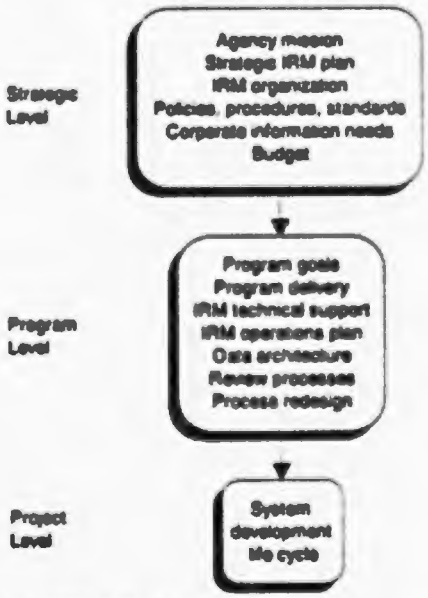

Figure 2. Stratification of the IRM Environment and Management Activities

Information Resources Management Planning Is Shaped by Management Perspective

IRM planning pervades *all* levels of agency management. At one level it may be perceived as a process of defining in a systematic way the information needed to effectively accomplish

---

[1] Information resources include hardware, software, data, and personnel; information systems; information assets maintained by the agency, such as reports, case files, electronic records, and data bases; document centers; information services, such as telecommunications services, computer services, and dissemination services.

agency missions and goals. At another level, it may be perceived as improving day-to-day information flows among related work processes for more efficient program results. And at yet another level, IRM practitioners may be intensely occupied in acquiring or developing technological capability to support end-users. As shown in Figure 2, IRM planning activities can be stratified according to three management perspectives: (1) strategic, (2) program, and (3) project. Even though all these IRM activities usually occur simultaneously and interactively, each perspective represents a particular arena of managerial focus within the broad field of IRM.

At the strategic level, IRM planning is generally associated with business planning and initiating, mandating, and facilitating process innovation and performance improvement. IRM is concerned with focusing technology investments on core business processes and business goals and establishing the IRM infrastructure needed to support the agency mission. Management is responsible for ensuring that the infrastructure exists and that it includes a variety of components, including (1) policies, procedures, and standards governing the development and use of information products and standards to support business goals, (2) IRM organization with clearly defined roles, responsibilities and accountability for information management; and (3) capability for building competence and motivation in human resources.

At the program level, IRM planning activities are shaped by (1) the need to manage program-critical information through all stages of the information life-cycle, (2) the deployment of computer-based systems to support program delivery, and (3) the reliance of program managers on IRM staff to develop computer-based systems. The planning function at this level is concerned with developing data and technology architectures, and providing support for day-to-day activities as well as redesign or modification of existing work processes or systems. Management is responsible for measuring performance and ensuring that current data flows, systems, and work processes are effectively supporting program goals and objectives. A program manager supported by an information system is responsible and accountable for cost-effective management of that system throughout its life-cycle.

At the project level, IRM planning activities are more narrowly confined to specific system acquisition and development projects. Planning at this level focuses on scheduling activities leading to project completion and installation of new or modified systems. Management is concerned with applying appropriate project oversight and control mechanisms. Management's responsibilities are to ensure that, throughout its life-cycle, the system under development (1) meets user requirements, (2) provides intended benefits to the agency and its constituencies, and (3) is developed on time and within budget. Figure 3 illustrates how the IRM perspective relates to the audit approach.

Just as IRM is shaped by the managerial perspective, so is the IRM audit approach shaped by that perspective. A general management review (GMR) would enter at the agency's strategic level of management. For example, the audit approach would consider agency-wide, high-level IRM activities that support the agency's mission, such as integration of IRM strategic

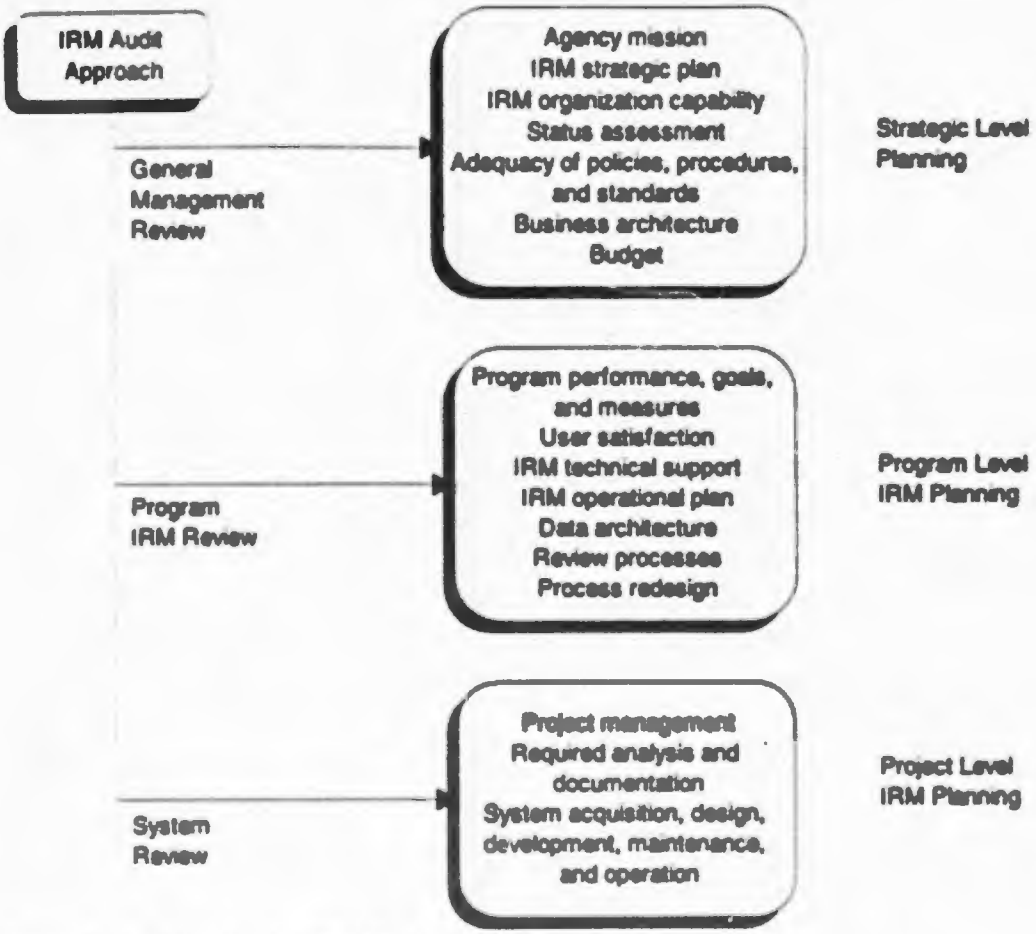

Figure 3 Auditing in the IRM Environment

planning with business planning; IRM organization and infrastructure; and IRM policies, standards, and procedures.

Entering at the program level of the agency, the IRM audit would focus on program-specific IRM issues. For example, some key questions to resolve would be whether current systems facilitate data sharing between or among interrelated programs, whether they satisfy user requirements and support program goals and objectives, and whether program managers are responsibly managing the development, operation, and maintenance of systems that support their programs. The program level is where one looks for the effects of technology on work processes, program delivery, and customer satisfaction.

If the audit were concerned with specific system development projects, then it would enter at the project level of agency activities. Key questions to be asked of the agency would be

predicated on where the agency believes it is in the development effort. For example, some key questions might be to ascertain whether user requirements have been adequately defined; whether system design specifications reflect user needs; whether the system being developed will meet those needs; and whether estimates of project costs, benefits, schedule, and installation resources are appropriately updated and revised throughout the life-cycle.

None of these levels is mutually exclusive. The auditor may have to work downward or upward to the next level when conditions manifest at one level but their causes originate at another.

IRM planning should be assessed from the standpoints of both the process and the plans resulting from the process. The process should be effectively supported, directed, and controlled by appropriate management mechanisms and should provide an opportunity for those affected by plans to participate in the process. The IRM plan and its component operational and systems development plans should clearly link IRM planning to business planning, look to the future by clarifying opportunities and threats that lie ahead for the agency, and provide a framework for decision-making and action.

The scope and depth of the IRM planning process varies according to the management level under consideration. In other words, planning at the strategic level should produce an IRM strategic plan; at the program level, an updated 5-year IRM operational plan; and at the project level, a system development action plan. Both strategic- and program-level planning are discussed in this part of the audit methodology. Project-level planning (i.e., system planning) begins the system development life-cycle, and is covered in The Concept Phase section of the audit guide.

BLANK PAGE

1.1 Strategic IRM Planning

In general, development of automated information systems should not occur outside of strategic IRM planning. In turn, strategic IRM planning cannot occur without a strategic "business" (or mission) plan for the organization. A strategic business plan systematically describes the agency's core business processes, constituencies or customers, their needs, the products and/or services that meet those needs, and the specific actions, responsibilities, and resource allocations necessary to satisfy the customers' needs over a projected period of time, generally at least 5 to 7 years in the future.

Ideally, strategic business planning and IRM planning are synchronized to occur simultaneously and interactively so that the impact of information resources on business outcomes is considered in the business planning process. However, the degree to which IRM planning and business planning are integrated or linked will depend on how much the CEO and the IRM official agree on the role of information and information technology in the agency on whether it is a support function or a strategic function.

Under ideal conditions, as business plans are formulated, the IRM official looks for targets of opportunity, weighing the influence of technological trends on business plans and suggesting alternative technological approaches to support future business scenarios. The selection and timing of new systems development projects are consistent with other business activities, and capital expenditures are made on the basis of business, not technology priorities.

In reality, few if any federal agencies have reached this level of integration. At best, federal agencies link strategic IRM planning to business plans that have been pulled together by program managers in support of the agency mission. More typically, however, the strategic business plan is in reality the budget documents prepared to support the agency's budget request to OMB and the Congress. The linkage between business planning and IRM strategic planning is generally reactive -- the business planning is done first, and the IRM official is asked to react to business plans in terms of what systems are needed to support them. For all practical purposes, IRM planning in federal agencies is represented by agency compliance with the 5-year information technology plan requirement contained in the Paperwork Reduction Act.

Strategic IRM planning should be an agency-wide, ongoing process of systematically obtaining and analyzing information about the agency's business, its future direction, critical success factors, and its current information systems environment. IRM planning ponders future changes in political environment, agency missions, and customer demand; it considers external and internal opportunities and threats; and various trends that may affect operations. Using this information IRM planners, working with program staff, can then link business functions to related information processes, and thus determine (1) what information is needed to achieve agency missions and program goals, and (2) the organization, specific

actions, technological approaches, time frames and other resource allocations necessary to satisfy the agency's information needs.

Audit Staffing Considerations

The audit steps discussed in all segments of this phase require a general understanding of strategic IRM planning concepts, including critical success factors, business systems planning, stage analysis, portfolio analysis, user needs surveys, architectural planning, and emerging technology applications. GAO program analysts knowledgeable in these areas should be included in the audit. Additionally, business process reengineering analysts and information system analysts will be required to assess or evaluate specific plans or other documents created in this phase.

Agency Profile

The audit steps in this part rely on the agency profile to provide information related to the inputs of the strategic planning process, particularly the mission of the agency and past and current problems in meeting the mission. Agency system profiles indicate how the agency is currently using information technology to meet its mission.

Outline of Segments

In this part of the planning phase, we are concerned with the agency's effectiveness in strategically defining the future results it desires, and in designing the methods for achieving them. This is accomplished in three segments of activity:

- Scope, definition, and organization. Identify mission-related issues and goals that will drive IRM planning and organize the planning process.
- Assessment of status and opportunity. Assess the strengths and weaknesses of current operations in light of the agency's mission and goals.
- Construct an IRM strategy. Define the IRM infrastructure and determine what strategy and approach the agency will take to change the current IRM environment so that it will better support current activities as well as new and emerging priorities.

1.1.1 Scope, Definition, and Organization Segment

The major risk associated with business planning and strategic IRM planning is that the agency's information resources may not support the agency's mission, goals, and objectives. To mitigate this risk, IRM planning should be integrated with the agency's program planning process, and effectively supported, directed, and controlled by appropriate management mechanisms. IRM planning should emphasize desired business outcomes rather than technology outcomes.

The agency should therefore establish the planning resources and processes necessary to integrate IRM planning with business planning for the agency. The process is a top-down approach by senior-level management to study the information needs of the agency; however, it requires bottom-up inputs from subagency operational-level staff. Management support, leadership, commitment, and accountability are critical elements to ensure that resources are effectively directed to completing the agency's business plan and the IRM strategic plan. The operative question to be answered in this segment is: How should we organize and what alternative approaches should we consider to improve the information products and services that support the agency's overall mission and program goals and objectives?

1.1.1.1 Agency Objectives for This Segment

1.1.1.1.1 Obtain executive-level management commitment, involvement, control, and accountability for the business and strategic IRM planning process.

1.1.1.1.2 Develop a business plan which identifies (1) core business (mission and program) issues, (2) issues that will shape or affect the IRM strategy and action plan, and (3) measures of performance for assessing whether customer needs are satisfied and business goals achieved.

1.1.1.1.3 Establish and organize the strategic IRM planning process; assign leadership and staff responsibilities to ensure that persons affected by the plan are formally and substantially involved in the process; and define the scope, objectives, and approach for the process.

1.1.1.1.4 Provide necessary training to members of the steering committee and planning team.

1.1.1.2 Relationship to Other Segments

The work performed in this segment lays the necessary groundwork, control environment, and organizational structure to ensure that strategic IRM plans appropriately support agency missions and objectives.

1.1.1.3 Agency Products and Documents Delivered During This Segment

1.1.1.3.1 A business plan which identifies (1) core business (mission and program) issues, (2) concerns that will shape or affect the IRM strategy and action plan, and (3) measures of performance for assessing whether customer needs are satisfied and business goals achieved.

1.1.1.3.2 A charter, identifying members of the IRM strategic planning team and defining responsibilities for integrating bottom-up and top-down strategic planning activities.

1.1.1.3.3 Documentation of key mission and program planning issues to be resolved/addressed during the IRM strategic planning process.

1.1.1.3.4 A work program or other documentation describing the schedule of planning milestones and management of checkpoints.

1.1.1.4 Management Responsibilities Discharged in This Segment

1.1.1.4.1 Communicate and guarantee commitment to and involvement in the planning process.

1.1.1.4.2 Appoint IRM planning team members (from both the program and IRM units) and define the charter and responsibilities of those involved, particularly the integration of mission and IRM strategies.

1.1.1.4.3 Define key mission and program planning issues and performance measures, as well as key management concerns and expectations.

1.1.1.4.4 Provide the planning team with leadership, including the necessary executive-level inputs, guidance, suggestions, and constructive criticism that will enhance the agency's planning process.

1.1.1.4.5 Review and approve the schedule of planning milestones and management checkpoints.

1.1.1.5 User Responsibilities Discharged in This Segment

1.1.1.5.1 Identify specific members (high-level program managers) to participate on the planning team.

1.1.1.5.2 Work with IRM staff to define strategic program-related issues to be addressed during the planning process, including issues of work-process redesign.

1.1.1.6 IRM Responsibilities Discharged in This Segment

1.1.1.6.1 Identify specific (high-level) members to participate on the planning team.

1.1.1.6.2 Work with users to help define strategic program-related issues to be addressed during the planning process.

1.1.1.7 Audit Objectives During This Segment

1.1.1.7.1 Assess whether the agency has developed a business plan which at least identifies:

a. core business (mission and program) issues;

b. issues that will shape or impact the IRM strategy and action plan; and

c. measures of performance for assessing whether customer needs are satisfied and business goals are achieved.

1.1.1.7.2 Assess whether the strategic IRM planning process is formally institutionalized through appropriate organizational structures, policies, and procedures, and whether:

a. responsibilities are clearly assigned;

b. the scope, objectives, and planning approach are established; and

c. necessary training is provided to the planning team and others involved in the planning process.

1.1.1.7.3 Assess whether the agency's strategic IRM planning process:

a. is integrated with business (mission) planning;

b. reflects agency-wide IRM policies, standards and procedures;

c. has senior-level management support;

d. provides top-down guidance to agency components; and

e. is effectively organized to include high-level representatives from agency management, program-level user groups, and IRM.

1.1.1.8 Audit Tasks for This Segment

1.1.1.8.1 Following the agency profile steps, compile and document appropriate background information, including the current status of the IRM environment pertinent to the agency program or activity to be audited. Current status information would include major information flows (data and reports) between information providers and information users and other information products and services supporting program goals and objectives.

1.1.1.8.2 Following the agency profile steps, review the report literature (i.e., congressional, prior GAO, Inspector General, internal audit, and Financial Integrity Act reports related to the program or activity and identify problem areas pertinent to the review).

1.1.1.8.3 Assess the agency's business plan (this may be their mission plan, management plan, budget document, etc.) to determine whether:

a. the agency identified the stated agency missions, goals, and objectives (of the activity or program to be audited);

b. goals and objectives are consistent with the agency's legislated mandates;

c. the agency has evaluated its business area and examined or developed new ways to address its core business issues;

d. business area analyses have impacted the IRM strategy and action plan; and

e. the agency has identified performance measures that will be used in assessing program effectiveness.

1.1.1.8.4 Assess the capability of the agency's planning organization. This can be done by obtaining information on:

a. the composition and skills of the planning team, and whether agency executive management considers the mix and number of personnel to be adequate and appropriate;

b. whether the team members have prior experience in performing planning activities and whether they have been successful in the past;

c. whether agency executive management has established a planning effort including senior representatives from user, policy, and IRM organizations affected by the plan; and

d. whether the IRM planning charter ensures that (1) agency-wide missions, goals, and objectives are properly reflected and incorporated into the planning process; (2) subagency-level plans are sufficiently comprehensive and complete; (3) subagency-level plans are not redundant or overlapping; and (4) the agency-wide plan, once approved, is implemented as scheduled.

1.1.1.8.5 Does the agency have policies and procedures for integrating IRM plans with agencywide business plans. (This integration might involve a 2-step process; i.e., combining all sub-agency level IRM plans into an overall IRM plan and then ensuring that the overall IRM plan is supportive of the agency-wide business plan.) Alternately, does the agency use information engineering methods for integrating information strategic planning with business area analysis with business and technical designs. Make a judgmental assessment of the integration process by looking for anomalies and inconsistencies in the application of these policies and procedures.

1.1.1.9 Audit Products and Work Papers Developed In This Segment

1.1.1.9.1 Copies of congressional, prior GAO, Inspector General, internal audit, and Financial Integrity Act reports related to the program or activity. Identify problem areas pertinent to the review.

1.1.1.9.2 Business plan or similar document(s) describing the agency's mission, goals, and program objectives, including legislative requirements and other mandates and directives for the programs within the scope of the review.

1.1.1.9.3 Work papers summarizing the auditor's assessment of the agency's business plan.

1.1.1.9.4 Work papers summarizing the auditor's review of the agency's planning capability including:

a. the composition, skills, and representation of the planning team and

b. the planning unit's charter, authority, and responsibilities.

1.1.1.9.5 Work papers assessing the effectiveness of the policies and procedures for integrating IRM plans with agency-wide business plans.

1.1.2 Status and Opportunity Assessment Segment

Before an agency can determine where it wants to go, it must first understand its current IRM infrastructure in terms of core business issues that may be affected by technology trends and that may impact IRM strategies. The purpose of this segment is to (1) identify opportunities to restructure core business activities, (2) identify ways in which the agency can better use information resources to support its mission and program objectives; and (3) assess technology trends and identify potential opportunities for using new technology. The operative questions to be answered in this segment are: *where are we, what is our condition, and what are the opportunities to improve our condition?*

1.1.2.1 Agency Objectives for This Segment

1.1.2.1.1 Understand the forces of the external environment (Congress, constituents, the public, etc.) which may influence or constrain the agency's planning process.

1.1.2.1.2 Identify the agency's mission, goals, and objectives and the information resources needed to support them effectively and efficiently.

1.1.2.1.3 In light of probable future scenarios, determine the strengths, weaknesses, and changeability of management and programmatic operation, and constituents' satisfaction with overall agency performance.

1.1.2.1.4 Assess the viability and capability of the current IRM infrastructure to support probable future scenarios.

1.1.2.1.5 Document major information technological and functional trends.

1.1.2.1.6 Define major IRM objectives to satisfy information needs in support of agency mission, goals, and objectives.

1.1.2.2 Relationship to Other Segments

This segment lays the groundwork necessary to develop IRM strategies for supporting future mission scenarios, organizational structures, and business processes.

1.1.2.3 Agency Products and Documents Delivered During This Segment

1.1.2.3.1 Description of external factors that may influence or constrain the agency's planning process.

1.1.2.3.2 Description of the agency's missions, goals, and objectives.

1.1.2.3.3 Analysis of the strengths and weaknesses of agency management, program operations, and overall agency performance in light of probable future scenarios.

1.1.2.3.4 Analysis of the impact and causes of any weaknesses or deficiencies that hinder the attainment of agency mission, goals, and objectives. This may take the form of an information strategic plan, a business area analysis, or an IG or a GAO report.

1.1.2.3.5 Description and assessment of IRM infrastructure to support probable future scenarios. This may be a business area analysis or business design in the case of information management systems.

1.1.2.3.6 Description of major information technology and functional trends.

1.1.2.3.7 Summary of major IRM objectives to satisfy information needs in support of agency mission, goals, and objectives.

1.1.2.4 Management Responsibilities Discharged in This Segment

1.1.2.4.1 Provide to the planning team a vision of the agency's probable future scenarios, including a clear statement of the agency's mission, goals, and objectives.

1.1.2.4.2 Identify and communicate to the planning team the IRM objectives that are needed to support the agency's strategic vision.

1.1.2.4.3 Provide executive-level inputs, guidance, suggestions, and constructive criticism to help the planning team assess current conditions and identify opportunities for improvement.

1.1.2.4.4 Help the planning team define the strategic management information needed to carry out the agency's overall mission, goals, and objectives.

1.1.2.4.5 Review results of status and opportunity assessment and provide consensus or approval before the planning team develops the IRM strategic plan.

1.1.2.5 User Responsibilities Discharged in This Segment

1.1.2.5.1 Assist the planning team in identifying the (1) strengths and weaknesses of programmatic operations and constituents' satisfaction with agency performance, (2) strengths and weaknesses of existing technological capabilities, and (3) IRM objectives for supporting the agency's strategic vision.

1.1.2.5.2 Assist the planning team in assessing the current IRM infrastructure and its potential capability for supporting the agency's vision.

1.1.2.6 IRM Responsibilities Discharged in This Segment

1.1.2.6.1 Assist the planning team in assessing (1) the current IRM infrastructure and its potential capability for supporting the agency's vision, and (2) the IRM objectives for supporting the agency's strategic vision.

1.1.2.6.2 Be alert to trends and identify new technologies that may be applied in support of the agency's vision.

1.1.2.7 Audit Objectives During This Segment

In this segment the auditor's objective is to understand how rigorously and effectively the agency has analyzed its current condition. Specifically, the auditor wants to know whether the agency has:

1.1.2.7.1 clearly identified and understood the demands and constraints of its external environment, and how these may affect the accomplishment of missions and goals;

1.1.2.7.2 identified strengths and weaknesses in its current IRM capabilities by analyzing its current processes and flow of data or information using business process reengineering methods;

1.1.2.7.3 systematically identified and categorized the information resources needed to achieve its stated missions and goals; and

1.1.2.7.4 identified major technological trends affording opportunities for improved mission performance.

1.1.2.8 Audit Tasks for This Segment

1.1.2.8.1 Determine whether the agency has identified the constraints of the external environment; review the agency's documentation of the impact of the external environment on mission performance.

1.1.2.8.2 Interview officials to determine whether the agency (i.e., IRM, program, quality assurance (QA), IG, or other unit) has assessed and documented the strengths and weaknesses of its IRM management practices and operations; obtain and evaluate documentation for all assessments made by the agency.

1.1.2.8.3 Determine whether the agency has adequately and clearly defined the IRM objectives to satisfy information needs in support of agency mission, goals, and objectives; review the agency's documentation to determine if the objectives are clearly and adequately stated and if they are appropriately linked to mission performance.

1.1.2.8.4 Determine whether the agency has assessed the strengths and weaknesses of its overall technological capability (by looking at the level of sophistication, adequacy to meet current user demands, and agency internal surveys); review the agency's documentation to determine the adequacy of its assessment.

1.1.2.8.5 Determine whether the agency has identified and documented major technology and functional trends and new opportunities for (a) using information technology, (b) reengineering functions and processes, or (c) using other resources to improve mission performance. If not, why not?

1.1.2.9 Audit Products and Work Papers Developed in This Segment

1.1.2.9.1 Documents summarizing external and internal reviews of agency mission and overall performance, IRM operations, and other activities related to the performance of agency missions and goals.

1.1.2.9.2 Work papers summarizing GAO analyses of:

a. comparison of stated mission with legislative requirements;

b. the relevance of the agency's information requirements to overall mission and program objectives, as well as the external environment;

c. budgets and related plans, including existing strategic, tactical, and operational plans;

d. the effectiveness of the agency's operations, including IRM mission-support activities; and

e. the agency's identification of opportunities for applying new technology and for reengineering current processes where warranted.

BLANK PAGE

1.1.3 IRM Strategy Segment

In this segment the agency determines its high-level IRM strategy and produces an IRM strategic plan. Ideally, the IRM strategy should be integrated with the agency's overall mission and program plan. The strategy should cover key information planning issues and technology alternatives that will satisfy management decision-making requirements as well as program operations requirements. These considerations should include cross-cutting technology management issues such as acquisition, computer security, internal controls, end-user computing, and telecommunications. The operative questions to be answered in this segment are: *Where do we want to be, and what resources are needed to get there?*

1.1.3.1 Agency Objectives for This Segment

1.1.3.1.1 Develop high-level IRM strategy reflecting (a) a 5 year to 7 year agency-wide view of how information resources are used to support the agency mission, goals, and objectives; and (b) any budgetary constraints.

1.1.3.1.2 Produce an IRM strategic plan that presents a vision of how IRM resources will be used to support the agency mission in the future, including an overall information architectural framework[2] that supports the selection, use, and integration of information resources within the agency.

1.1.3.1.3 Obtain management review and approval of the IRM strategy and strategic plan.

1.1.3.2 Relationship to Other Segments

This segment summarizes the results of the status and opportunity assessment segment, and lays out an integrated strategy and architectural framework for improving agency operations. The work performed here is prerequisite to producing a program-level, operational action plan.

---

[2] An architecture is a map of the agency's information requirements showing (1) how major information categories relate to agency processes and how they must be integrated and shared to support the agency's mission, goals, and objectives; and (2) how the various technological components (e.g., computers, peripherals, networks) are located and interconnected to pass information from one functional area to another.

1.1.3.3 Agency Products and Documents Delivered During This Segment

1.1.3.3.1 IRM strategic plan that provides at a minimum, a 5 year to 7 year projection of major functions and operations of the agency. The plan should at least include the following elements:

a. a mission statement for major functions and operations;
b. general goals and objectives and how they are to be achieved;
c. operational resources (including information resources) required to meet the goals and objectives;
d. a schedule for implementing proposed new program initiatives; and a description of the organizational and operational impacts of these initiatives.
e. performance goals and measures;
f. an architectural framework;
g. key external factors that could affect the achievement of goals and objectives; and
h. a schedule for future program evaluations and planning adjustments.

1.1.3.3.2 Summary of the agency's budget, including preliminary program-level IRM budgets.

1.1.3.4 Management Responsibilities Discharged in This Segment

1.1.3.4.1 Provide final executive-level comments, guidance, suggestions, and constructive criticism to help the planning team complete the IRM strategy and strategic plan.

1.1.3.4.2 Ensure that the IRM strategic plan is consistent with and linked to the agency business plan and to the budget.

1.1.3.4.3 Review and approve the IRM strategy and strategic plan.

1.1.3.5 User Responsibilities Discharged in This Segment

1.1.3.5.1 Assist the planning team in formulating proposed IRM strategies and developing the strategic plan.

1.1.3.5.2 Assist the planning team in presenting the proposed strategies and plan to management, including a description of the impacts that the plan will have on program-level operations and on the accomplishment of the agency's current mission (such as the ability to deliver services, organizational restructuring, return on investment, personnel reductions, and reengineering of work processes).

1.1.3.6 IRM Responsibilities Discharged in This Segment

1.1.3.6.1 Assist the planning team in formulating proposed IRM strategies and developing the strategic plan.

1.1.3.6.2 Assist the planning team in presenting the proposed strategies and plan to management, including a description of the impacts that the plan will have on program-level operations and on the accomplishment of the agency's current mission (such as the ability to deliver services, organizational restructuring, return on investment, personnel reductions, and reengineering of work processes).

1.1.3.7 Audit Objectives During This Segment

1.1.3.7.1 Determine whether the agency has developed an IRM strategy and strategic plan.

1.1.3.7.2 Determine whether the agency's strategic IRM plan can serve as a useful decision-making framework and whether it is comprehensively and adequately developed.

1.1.3.7.3 Determine whether executive management has approved the IRM strategy and strategic plan

1.1.3.8 Audit Tasks for This Segment

1.1.3.8.1 Review the agency's plans and related planning documentation and assess whether the agency (1) established governing strategies for identifying and managing information resources within the agency, including agencywide IRM goals, overall assumptions, and constraints; and (2) provided these strategies to program-level units for their use in developing their components of the IRM strategic plan.

1.1.3.8.2 Determine whether the executive management and the designated IRM official have reviewed and approved strategic plan submissions from the subagency-level units to ensure compliance with the strategies and agencywide goals.

1.1.3.8.3 Determine whether the strategic IRM plan includes the following critical elements:

a. a mission statement for major functions and operations;
b. general goals and objectives and how they are to be achieved;
c. operational resources (including information resources) required to meet the goals and objectives;
d. a schedule for implementing proposed new program initiatives and a description of the organizational and operational impacts of these initiatives.
e. performance goals and measures;
f. an architectural framework;
g. key external factors that could affect the achievement of goals and objectives; and
h. a schedule for future program evaluations and planning adjustments.

1.1.3.8.4 Review the agency's IRM strategy and strategic plan and decide whether it can drive decision-making for investing in future information resources needed to accomplish agency mission, goals, and objectives.

1.1.3.8.5 Determine whether the IRM strategic plan is linked to the agency's budget, including preliminary program-level IRM budgets.

1.1.3.8.6 Determine whether the IRM strategies adequately consider what must be done to transition smoothly from the old IRM environment to the new.

1.1.3.8.7 Determine whether senior management has reviewed and approved the IRM strategy and strategic plan.

1.1.3.9 Audit Products and Work Papers Developed in This Segment

1.1.3.9.1 The agency's IRM strategic plan and other planning-related documentation, including architectures and related budget documents.

1.1.3.9.2 Work papers assessing whether:

a the agency established governing strategies for identifying and managing information resources within the agency, including agencywide IRM goals, overall assumptions, alternative choices, and constraints;

b. these strategies were provided to program-level units for their use in developing their components of the IRM strategic plan;

c. the strategic IRM plan includes all the critical elements;

d. the plan can drive decision-making for investing in future information resources needed to accomplish agency mission, goals, and objectives;

e. the IRM strategic plan is linked to the agency's budget including preliminary program-level IRM budgets;

f. the IRM strategies adequately consider what must be done to transition smoothly from the old IRM environment to the new; and

g. senior management has reviewed and approved the IRM strategy and strategic plan.

1.1.3.9.3 Documentation of the senior executive's and the designated IRM official's review and approval of the strategic plan.

BLANK PAGE

1.2 Program-Level IRM Planning

IRM planning at this level is defined by OMB as "operational" planning. The process considers more immediate IRM issues to meet anticipated program and mission needs, usually focusing on IRM activities and projects over a 1- to 5-year planning horizon. In general, this type of planning seeks opportunities to (1) improve program delivery and program administration by first redesigning work processes and then judiciously applying information technology; (2) manage information throughout its life-cycle to maximize its usefulness, including intra- and inter-agency sharing of data; (3) minimize the information collection burden imposed by the agency on the public; and (4) preserve the integrity, availability, and confidentiality of information. The operative questions to be answered at this level are: *What tasks do we need to do, and in what priority, to get where we want to go?*

Plan Contents

Planning at this level should result in an annually updated 5-year plan, as required by 44 USC 3506, which includes the specific actions to be taken toward accomplishing the IRM strategies documented in the IRM strategic plan. The plan would include a listing of technology projects approved by management to support users and program managers in moving from the current to the future IRM environment and it would identify the sequence of actions the agency must follow to implement these projects. For the projects identified, the costs and benefits are approximated to determine the feasibility of each project. For each project, the plan should also cover (1) a summary of the agency's functional requirements and information needs, including key characteristics of present and planned applications; (2) new organizational structures, management practices, and human resource requirements; (3) architectures for computer hardware and software, data, and communications; and (4) security requirements.

Risk Management

The primary risk associated with program-level IRM planning is that the agency's program objectives may not be adequately supported by its information resources. Controls to mitigate this risk include executive management commitment and support; appropriate oversight mechanisms; enforcement of policies, procedures, and standards; adequate user involvement in the planning process; and periodic IRM and system plan reviews.

Audit Staffing Considerations

The audit steps discussed in all segments of this phase require a general understanding of

IRM concepts, architectural planning, federal requirements for preparation and submission of budget estimates, and cost-benefit analyses. In those cases where cost and schedule estimates have been developed by the agency, a technical specialist knowledgeable in formal cost and scheduling methods may be required to assess the validity of the development approach and the estimates themselves.

Additional Considerations

Personnel at the program operations level may tend to be satisfied with current information and systems; however, the planning team is responsible for identifying technological advances and functional trends which, though not recognized by operational personnel, may improve the program unit's operations. The planning team may also identify opportunities for reengineering work processes to significantly improve program operations.

Agency Profile

Audit steps in this part rely on the agency profile to provide information on the organization of the agency, applicable standards, policies and procedures, strengths and weaknesses of its operations, and its current IRM capability.

Outline of Segments

In this part of the planning phase, we are concerned with the agency's effectiveness in defining its operational requirements for information resources, including technical architectures to support agency programs. This is accomplished in three segments of activity:

- *Scope, definition, and organization.* Identify program-related issues and goals that will drive IRM planning, and organize the planning process.
- *Assessment of status and opportunity.* Assess the strengths and weaknesses of current program operations in light of the agency's mission and goals.
- *Construct an IRM operational plan.* Define the IRM infrastructure and determine what approach the agency will take to change the current IRM environment so that it will better support current program activities as well as new and emerging priorities.

1.2.1 Scope, Definition, and Organization Segment

The agency needs to establish the planning resources and processes necessary to integrate IRM planning with business or program planning. Management support, leadership, and commitment are critical elements to ensure that resources are effectively directed to completing the IRM operational plan. The operative question to be answered in this segment is: *How should we organize and what alternative approaches should we consider to improve the information systems, products, and services that support the agency's mission?*.

1.2.1.1 Agency Objectives for This Segment

1.2.1.1.1 Obtain program management's commitment, involvement, control, and accountability for the planning process.

1.2.1.1.2 Establish and organize IRM operational planning and assign leadership and staff responsibilities to ensure that persons affected by the operational plan are formally and substantially involved in the planning process.

1.2.1.1.3 Define the scope, objectives, and approach for the IRM planning process and identify business issues (program goals and objectives) and concerns that will shape or impact the IRM operational plan.

1.2.1.1.4 Provide necessary training to members of the planning team.

1.2.1.1.5 Plan a quality assurance and system configuration management (including documents) process that supports the mission and program objectives.

1.2.1.2 Relationship to Other Segments

The work performed in this segment lays the necessary groundwork, control environment, and organizational structure to ensure that IRM operational plans appropriately identify specific IRM projects to support program missions and objectives.

1.2.1.3 Agency Products and Documents Delivered During This Segment

1.2.1.3.1 Charter for the program planning team identifying members and defining responsibilities for integrating the agency's IRM plans with program goals and objectives.

1.2.1.3.2 A listing of key mission and program planning issues to be resolved/addressed during the planning process.

1.2.1.3.3 A work program including a schedule of planning milestones and management checkpoints.

1.2.1.4 Management Responsibilities Discharged in This Segment

1.2.1.4.1 Communicate and guarantee commitment to and involvement in the planning process.

1.2.1.4.2 Appoint IRM planning team members and define the charter and responsibilities of those involved, particularly the integration of program goals and objectives with IRM plans.

1.2.1.4.3 Define key mission and program planning issues (e.g., work process redesign, quality assurance and control, configuration management) and performance measures, as well as key management concerns and expectations.

1.2.1.4.4 Review and approve the planning schedule and work program.

1.2.1.5 User Responsibilities Discharged in This Segment

1.2.1.5.1 Identify specific members to participate on the planning team.

1.2.1.5.2 Work with IRM staff to define program-level operational issues to be addressed during the planning process.

1.2.1.6 IRM Responsibilities Discharged in This Segment

1.2.1.6.1 Identify specific members to participate on the planning team.

1.2.1.6.2 Work with users to help define program-level operational issues to be addressed during the planning process.

1.2.1.7 Audit Objectives During This Segment

1.2.1.7.1 Assess whether the agency has developed a strategic plan which at least identifies:

a. mission and program issues;

b. issues that will shape or impact the IRM operational plan;

c. measures of performance for assessing whether customer needs are satisfied and program goals are achieved.

1.2.1.7.2 Assess whether the IRM operational planning process is formally institutionalized through appropriate organizational structures, policies, and procedures, and whether:

a. responsibilities are clearly assigned;

b. the scope, objectives, and planning approach are established; and

c. necessary training is provided to the planning team and others involved in the planning process.

1.2.1.7.3 Assess whether the agency's operational IRM planning process:

a. is integrated with program planning;

b. reflects agency-wide IRM policies, standards and procedures;

c. has program-level management support;

d. provides top-down guidance to program components; and

e. is effectively organized to include representatives from program-level management, user groups, and IRM

1.2.1.8 Audit Tasks for This Segment

1.2.1.8.1 Following the agency profile steps, compile and document appropriate background information, including the current status of the IRM environment pertinent to the agency program or activity to be audited. Current status information would include major information flows (data and reports) between information providers and information users and other information products and services supporting program goals and objectives.

1.2.1.8.2 Following the agency profile steps, review the report literature (i.e., congressional, prior GAO, Inspector General, internal audits, and Financial Integrity Act reports related to the program or activity, and identify problem areas pertinent to the review.

1.2.1.8.3 Assess the agency's strategic IRM plan to determine whether the agency:

a. identified the stated agency missions, goals, and objectives pertinent to the program to be audited;

b. whether program goals and objectives are consistent with the agency's legislated mandates;

c. has identified mission and program issues that will impact the IRM operational plan.

1.2.1.8.4 Assess the capability of the agency's planning organization. This can be done by obtaining information on:

a. the composition and skills of the planning team and whether agency executive management considers the mix and number of personnel to be adequate and appropriate;

b. whether the team members have prior experience in performing planning activities and whether they have been successful in the past;

c. whether program management has established a planning effort including program-level representatives from user, policy, and IRM organizations affected by the IRM operational plan; and

d. whether the IRM planning charter ensures that (1) agencywide missions, goals, and objectives are properly reflected and incorporated into the planning process; (2) program-level plans are sufficiently comprehensive and complete; (3) program-level plans are not redundant or overlapping; and (4) the agencywide plan, once approved, is implemented as scheduled.

1.2.1.8.5 Does the agency have processes and mechanisms for integrating program-level business and IRM plans and linking them to strategic IRM and agency-wide business plans and the budget? If yes, make a judgmental assessment by looking for anomalies and inconsistencies in the application of these processes.

1.2.1.9 **Audit Products and Work Papers Developed in This Segment**

1.2.1.9.1 Documents describing the agency's mission, goals, and program objectives, including legislative requirements and other mandates and directives for the programs within the scope of the review.

1.2.1.9.2 Copies of congressional, prior GAO, Inspector General, internal audit, and Financial Integrity Act reports related to the program or activity, identifying problem areas pertinent to the review.

1.2.1.9.3 Work papers summarizing the auditor's assessment of the agency's strategic IRM plan (assuming that the strategic IRM plan is a prerequisite input to scoping the operational planning process).

1.2.1.9.4 Work papers summarizing the auditor's review of the agency's planning capability including:

a. the composition, skills, and representation of the planning team;

b. the executive management charter, makeup, authority, and responsibilities.

1.2.1.9.5 Work papers assessing the effectiveness of the processes and mechanisms for integrating program-level business and IRM plans and linking them to strategic IRM and agencywide business plans.

BLANK PAGE

1.2.2 Status and Opportunity Assessment Segment

The program organization needs to determine whether it is using information and information technology in the most effective way to achieve program goals and objectives and serve its customers. It needs to assess its current IRM environment not only in terms of operational effectiveness and efficiency, but also in terms of (1) identifying the information products and services the program organization needs to serve its customers, and (2) finding opportunities to improve service delivery by redesigning work processes and exploiting technology trends. The operative questions to be answered in this segment are: *Where are we, what is our condition, and what are the opportunities to improve our condition?*

1.2.2.1 Agency Objectives for This Segment

1.2.2.1.1 Understand the forces of the external environment (budget, Congress, constituents, the public, etc.) which may influence or constrain the agency's planning process.

1.2.2.1.2 Determine the impact and causes of any weaknesses or deficiencies that impede the attainment of program goals and objectives.

1.2.2.1.3 Assess user/customer satisfaction with existing information systems, services, and products and establish measures of performance.

1.2.2.1.4 Identify ways to better use information resources to support program goals and objectives and satisfy customers, including opportunities to redesign work processes.

1.2.2.1.5 Identify the information products, services, and resources needed to support program goals and objectives effectively and efficiently.

1.2.2.1.6 Assess current IRM technical support operations, technical architecture, and capacity.

1.2.2.1.7 Assess the skills, practices, and organization of the IRM community to determine its effectiveness in supporting program goals and objectives.

1.2.2.1.8 Document and assess technology trends and identify opportunities for using new technology to improve program operations as well as service delivery.

1.2.2.1.9 Define major IRM objectives to satisfy information needs in support of program goals and objectives.

1.2.2.2 Relationship to Other Segments

This segment lays the groundwork necessary to develop the IRM operational plan.

1.2.2.3 Agency Products and Documents Delivered During This Segment

1.2.2.3.1 Description of the agency's mission, goals, and objectives; and its external environment.

1.2.2.3.2 Analysis of the impact and causes of any weaknesses or deficiencies that hinder the attainment of agency mission, goals, and objectives.

1.2.2.3.3 Description and assessment of user/customer satisfaction with existing information systems, services, and products, including performance measures.

1.2.2.3.4 Description of new ways and approaches to better use information resources to fulfill program goals and objectives, including opportunities for work process redesign.

1.2.2.3.5 Description of information products, services, and resources needed to support program goals and objectives.

1.2.2.3.6 Analysis of current IRM technical support operations, technical architecture, and capacity.

1.2.2.3.7 Description and assessment of IRM organization's skills, practices, organization, and capabilities.

1.2.2.3.8 Description of major information technology trends and opportunities for using new technology for improved program operations as well as service delivery.

1.2.2.3.9 Definition of criteria for establishing priorities among systems development projects.

1.2.2.4 Management Responsibilities Discharged in This Segment

1.2.2.4.1 Provide a clear statement of the agency's mission, goals, and objectives.

1.2.2.4.2 Provide the planning team with inputs from program managers, including priority-setting criteria, guidance, suggestions, and constructive criticism.

1.2.2.4.3 Identify and communicate to the planning team the management information needed to manage program operations and activities, including information needed to measure program performance.

1.2.2.4.4 Review results of status and opportunity assessment and provide consensus or approval before the planning team begins work on the next segment.

1.2.2.5 User Responsibilities Discharged in This Segment

1.2.2.5.1 Assist the planning team in identifying the (1) strengths and weaknesses of existing technological capabilities and (2) information products, systems, and services needed to accomplish program goals and objectives and satisfy customer needs.

1.2.2.5.2 Identify the extent to which current systems and functional processes meet user needs, and identify opportunities for work process redesign and improvement of program operations.

1.2.2.5.3 Assist the planning team in assessing the skills, practices, and organization of user groups to determine (1) their effectiveness in servicing customers and supporting program goals and objectives and (2) requirements for training and support.

1.2.2.6 IRM Responsibilities Discharged in This Segment

1.2.2.6.1 Assist the planning team in identifying the current status of and potential improvements to program applications of information technology, and identify opportunities for work process redesign and improving program operations.

1.2.2.6.2 Be alert to trends, and identify new technologies that may be applied in support of agency operations.

1.2.2.6.3 Assist the planning team to define major information technology objectives that satisfy information needs.

1.2.2.6.4 Assist the planning team in assessing the skills, practices, and organization of the IRM community to determine (1) their effectiveness in servicing users and supporting program goals and objectives and (2) requirements for training and support.

1.2.2.7 Audit Objectives During This Segment

Determine whether the agency has effectively established a baseline and framework for improving program delivery and IRM support of program operations by clearly identifying and articulating:

1.2.2.7.1 the demands and constraints of its external environment, and how these may affect the accomplishment of missions and goals;

1.2.2.7.2 the strengths and weaknesses in its current IRM capabilities that may enhance or impede attainment of program goals and objectives;

1.2.2.7.3 user/customer demands for improved information systems, services, and products and criteria by which program performance and IRM support can be measured;

1.2.2.7.4 better ways to use information resources to support program goals and objectives and satisfy customers, including opportunities to re-design work processes;

1.2.2.7.5 the information products, services, and resources needed to support program goals and objectives;

1.2.2.7.6 the strengths and weaknesses of current IRM technical support operations, technical architecture, and capacity;

1.2.2.7.7 the strengths and weaknesses of the IRM organization's skills, practices, organization, and capabilities;

1.2.2.7.8 the major information technology trends and the opportunities for using new technology for improved program operations as well as service delivery; and

1.2.2.7.9 the criteria for establishing priorities among planned systems development projects.

1.2.2.8 Audit Tasks for This Segment

1.2.2.8.1 Review the agency's documentation and determine whether the agency has effectively identified and described the constraints of its external environment, and how these may affect the accomplishment of missions and goals.

1.2.2.8.2 Review agency documentation and assess whether the agency has adequately and clearly defined the IRM objectives to satisfy information needs in support of program goals and objectives.

1.2.2.8.3 Interview users/customers, review agency documentation, and assess whether the agency has (a) obtained feedback from the user community on the sufficiency of IRM support to program operations and (b) clearly identified and articulated user/customer demands for improved information systems and services.

1.2.2.8.4 Interview the user community, review agency documentation, and determine the adequacy of the agency's identification of better ways to use information resources to support program goals and objectives, including opportunities to redesign work processes.

1.2.2.8.5 Review the documentation and determine whether the agency has adequately identified the information products, services, and resources needed to support program goals and objectives.

1.2.2.8.6 Determine whether the agency has identified the strengths and weaknesses of current IRM technical support operations, technical architecture, and capacity; and review the documentation to determine the adequacy of the agency's assessment.

1.2.2.8.7 Determine whether the agency has identified the strengths and weaknesses of the IRM organization's skills, practices, organization, and capabilities and review the documentation to determine the adequacy of the agency's assessment.

1.2.2.8.8 Determine if the agency has identified the major information technology trends and the opportunities for using new technology for improved program operations as well as service delivery; and review the documentation to determine the adequacy of the agency's assessment.

1.2.2.8.9 Determine whether the agency has documented the criteria for establishing priorities among planned systems development projects;

review the documentation and determine whether the criteria are adequate and relevant to program goals and objectives.

1.2.2.9 Audit Products and Work Papers Developed in This Segment

1.2.2.9.1 Documents summarizing external and internal reviews of program mission and overall performance, IRM activities in support of program operations, and other activities related to the performance of the accomplishment of program goals and objectives.

1.2.2.9.2 Work papers summarizing GAO analyses of:

a. a comparison of program goals and objectives with stated agency mission and legislative requirements;

b. the relevance of the agency's information requirements to overall mission and program objectives, as well as the external environment;

c. the agency's assessment of the strengths and weaknesses of its current IRM capabilities and their impacts on the attainment of program goals and objectives;

d. budgets and related plans, including existing strategic, tactical, and operational plans;

e. user/customer views and feedback concerning needs for improved information systems, services, and products;

f. agency criteria for measuring program performance, and the effectiveness of IRM support;

g. the effectiveness of the agency's operations, including IRM technical support activities; IRM unit's skills, practices, organization, and capabilities;

h. the agency's identification of opportunities for applying new technology and for reengineering current processes where warranted; and

i. the agency's criteria for establishing priorities among planned systems development projects.

1.2.3 IRM Strategy Segment

In this segment the program unit produces an operational IRM plan. The operational plan should cover key information planning issues and technology alternatives that will satisfy management decision-making requirements as well as program operations requirements. All of the work performed in the preceding segments is finalized and integrated into a cohesive operational plan document.

The cost-benefit relationships of all required projects are approximated to determine feasibility. Feasible projects and strategies will not require more resources than management is willing to allocate. If the overall assessment reveals that adequate resources may not be available, the strategies may be revised and the process repeated. After the planning team assembles the IRM Operational Plan, it is reviewed by IRM and program management to verify that it addresses the key planning issues and the IRM objectives. These considerations should include cross-cutting technology management issues such as acquisition, computer security, internal controls, end-user computing, and telecommunications. The plan is then presented to top management for approval. The operative questions to be answered in this segment are: *What changes do we want to make and what resources are needed to make them?*

1.2.3.1 Agency Objectives for This Segment

1.2.3.1.1 Develop, for inclusion in the IRM Operational Plan, an implementation strategy that groups and prioritizes action items into projects that will achieve the IRM objectives. (Note: For all intents and purposes, the implementation strategy document created is likely to be the 5-year "Information Technology Plan" required under Section 3506 of the Paperwork Reduction Act.)

1.2.3.1.2 Produce an IRM operational plan that will describe how IRM resources will be used to support program goals and objectives, including an overall architectural framework that supports the selection, use, and integration of information resources within the agency.

1.2.3.1.3 Obtain management review and approval of the IRM operational plan.

1.2.3.2 Relationship to Other Segments

This segment summarizes the results of the status and opportunity assessment segment and lays out an integrated strategy and operational plan for improving program operations.

1.2.3.3 Agency Products and Documents Delivered During This Segment

1.2.3.3.1 IRM operational plan that prioritizes projects that will achieve IRM objectives over 2-3 years, and describes how IRM resources will be used to support program goals and objectives, including the overall architectural framework.

1.2.3.3.2 Preliminary cost-benefit analysis and/or alternatives analysis for each major project summarized in the operational plan.

1.2.3.3.3 Preliminary IRM budget for each major project summarized in the operational plan.

1.2.3.4 Management Responsibilities Discharged in This Segment

1.2.3.4.1 Provide final comments, guidance, suggestions, and constructive criticism to help the planning team complete the IRM implementation strategy and operational plan.

1.2.3.4.2 Ensure that the IRM operational plan is consistent with and linked to the IRM strategic and agency business plans.

1.2.3.4.3 Review and approve the IRM implementation strategy and operational plan.

1.2.3.5 User Responsibilities Discharged in This Segment

1.2.3.5.1 Assist the planning team in formulating the IRM implementation strategy and developing the operational plan.

1.2.3.5.2 Assist the planning team in presenting the proposed strategies and plan to program management, including a description of the impact that the plan will have on (1) program operations and on the accomplishment of program goals and objectives, and (2) the ability to deliver services, organizational restructuring, return on investment, personnel reductions, and reengineering of work processes.

1.2.3.6 IRM Responsibilities Discharged in This Segment

1.2.3.6.1 Assist the planning team in formulating the IRM implementation strategy and developing the operational plan.

1.2.3.6.2 Assist the planning team in presenting the proposed strategies and plan to program management, including a description of the impact that the plan will have on (1) program operations and on the accomplishment of program goals and objectives, and (2) the ability to deliver services, organizational restructuring, return on investment, personnel reductions, and reengineering of work processes.

1.2.3.7 Audit Objectives During This Segment

1.2.3.7.1 Determine whether the agency has developed an IRM implementation strategy and operational plan. This includes reviewing the initial operating capability (IOC) and full deployment strategies.

1.2.3.7.2 Determine whether the agency's IRM operational plan can serve as a basis for implementing changes to agency programs and IRM support activities.

1.2.3.7.3 Determine whether the IRM operational plan is consistent with and linked to the IRM strategic and agency business plans.

1.2.3.7.4 Determine whether program management has approved the IRM implementation strategy and operational plan.

1.2.3.8 Audit Tasks for This Segment

1.2.3.8.1 Review the IRM operational plan, and determine whether it includes an implementation strategy that groups and prioritizes action items into projects that will achieve the IRM objectives; assess the plan for completeness of coverage and depth of implementation details.

1.2.3.8.2 Assess whether the IRM operational plan adequately describes how IRM resources will be used to support program goals and objectives, including an overall architectural framework that supports the selection, use, and integration of information resources within the agency.

1.2.3.8.3 Interview key officials and review agency records to determine whether management reviewed and approved the IRM operational plan; determine whether these officials have properly accepted accountability for implementing the plan.

1.2.3.8.4 Review the plan, budget, and related documentation to determine whether the IRM implementation strategy and operational plan are

adequately supported by funding included the in agency's budget; determine whether multi-year funding is likely to be continued for implementation projects to ensure their completion.

1.2.3.8.5 Review the plan and related documentation and interview key officials to determine whether the IRM implementation strategy adequately and systematically considers what must be done to implement the projects and transition smoothly from the old IRM environment to the new.

1.2.3.9 Audit Products and Work Papers Developed in This Segment

1.2.3.9.1 The agency's IRM operational plan, including the implementation strategy, budgets, cost-benefit and/or alternatives analyses, architectures, and other planning-related documentation.

1.2.3.9.2 Work papers documenting whether:

a. the IRM operational plan includes an implementation strategy that groups and prioritizes action items into projects that will achieve the IRM objectives;

b. the IRM Operational Plan is complete in coverage and depth of implementation details;

c. the IRM operational plan adequately describes how IRM resources will be used to support program goals and objectives, including an overall architectural framework that supports the selection, use, and integration of information resources within the agency;

d. management has reviewed and approved the IRM operational plan and whether these officials have properly accepted accountability for implementing the plan;

e. the IRM implementation strategy and operational plan are adequately supported by funding included in the agency's budget; and whether multi-year funding is likely to be continued for implementation projects to ensure their completion; and

f. the IRM implementation strategy adequately and systematically considers what must be done to implement the projects and transition smoothly from the old IRM environment to the new.

Contents of the Concept Phase

2.0 The Concept Phase

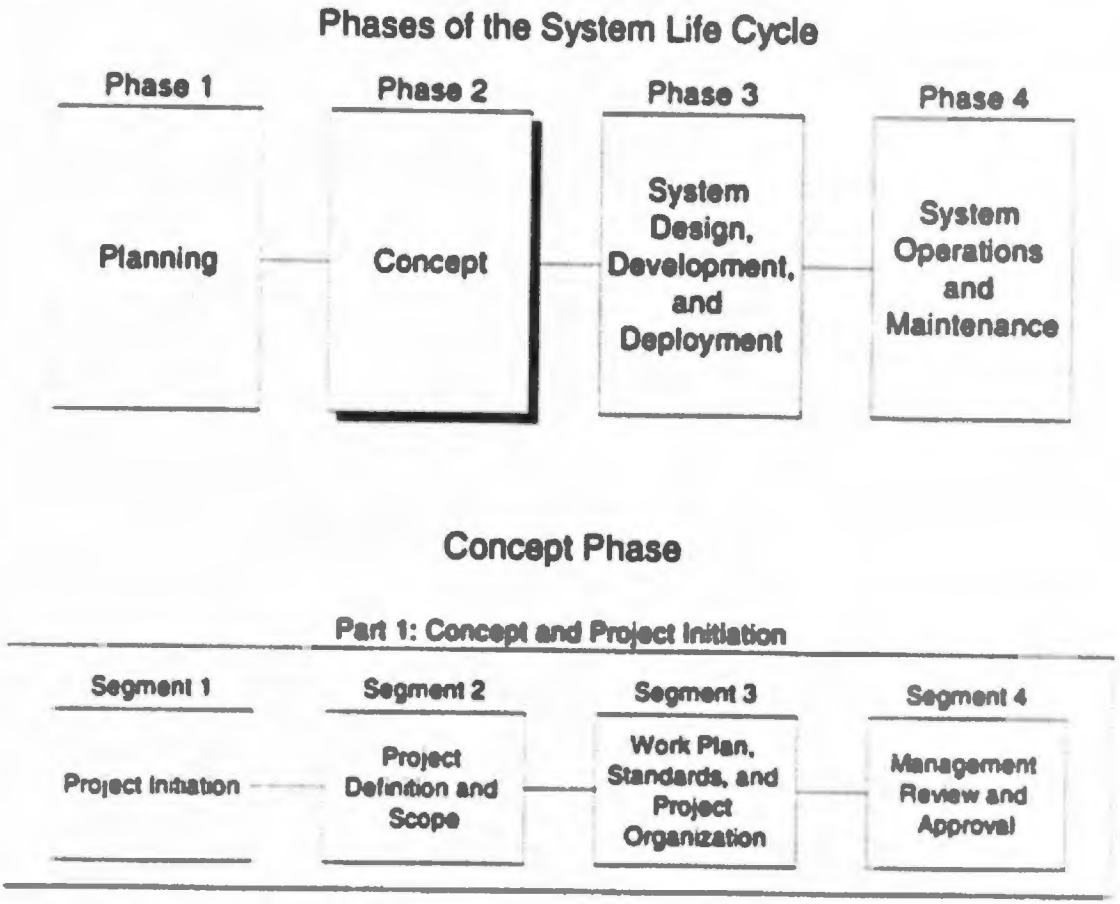

Figure 4. The Concept Phase

BLANK PAGE

2.1 Concept and Project Initiation

From an agency perspective, the purpose of this phase is to identify and evaluate alternative functional and technical concepts that satisfy an approved set of requirements (this may be referred to as a mission needs statement). The fundamental premise underlying this phase of the AIS life-cycle is that there are either legacy systems that require corrective action or new capabilities, or new or replacement systems are required so as to better satisfy the agency's mission.

In this phase, it is important that the evaluation team determine if the agency has developed alternative concepts of operation that it is analyzing. At this point, the evaluation team may have to perform structured walkthroughs of the agency process, or perform a formal business area analysis (including process modeling, activity modeling, and/or data modeling, if necessary) to deduce the existing method of operation and its characteristics. If the agency has already performed such an analysis then the evaluation team may have to verify the model developed by the agency and the results derived from the model. Such a verification would have to include the accuracy and completeness of the agency data used in the model.

Furthermore, issues related to transitioning from existing legacy or problem systems to modernized systems needs to be addressed as part of the risk management process. The concept of operation must include refinements to the strategies developed in the planning phase for overcoming impediments such as budgetary, political, cultural, and technical constraints.

After the agency has completed its information planning process it is ready to begin project-level planning activities; that is, developing the high-priority projects identified in the IRM Operational Plan that was approved by the agency during its planning activities. This phase consists of approving and initiating a system development project, developing a system concept, and planning and organizing the necessary tasks for designing and developing the system.

Project Planning

Project-level planning enables IRM managers to avoid duplication of resources, and minimize, if not eliminate cost overruns and other problems associated with performing complex tasks that must be well-coordinated, accomplished over extended timeframes, and inclusive of many people. A project plan may be as simple as a Gantt chart that identifies tasks, task responsibilities, and project start and end times, or it may involve more sophisticated techniques such as PERT that might include such features as assignment of support resources, task dependencies, critical path identification, and cost itemization by task. All such plans allow managers the opportunity to compare actual progress to planned events.

As a practical matter, project-level planning establishes a detailed action plan and goals to meet objectives of specific systems for program units or divisions under common control or authority, rather than for the entire agency. Customarily, these activities are completed in four segments:

-- Project Initiation. From the strategy developed in the planning phase, the Work or Action Plan to improve program or system performance is developed. Management approves a development project and establishes a project team to initiate it after taking into consideration the impediments and budgetary constraints that apply.

-- Project Definition and Scope. The project team develops a system concept (a general description of the major components of the system and how they work together to meet users' needs that address acknowledged deficiencies in program and/or system performance.

-- Work Plan, Standards, and Project Organization. The project team defines an organizational structure for designing and developing the project, develops a work plan, and sets standards for the project.

-- Management Review and Approval. Management reviews the project team's proposals regarding changes to business operations, organizational barriers or impediments, and systems installation with minimum disruption to existing operations before deciding to enter the design phase.

Risk Management

A risk management plan is used to minimize the risk of project failure by effectively applying controls to mitigate the likelihood of loss from certain events. In systems development projects, risk is exposure to adverse consequences such as (1) schedule or budget overruns; (2) failure to meet user expectations or address acknowledged deficiencies in existing systems; (3) continuing to spend money to complete projects even after it is apparent that the project is defective or is no longer cost effective; and (4) project development is proceeding on schedule and within budget but because of a change in mission the project no longer contributes to the organization's goals. The project manager must be concerned with two facets of risk: business risk and project risk.

Business risk. Business risk arises from a combination of one or more of the following factors: not doing one or more projects, not having the correct processes, systems, or staff skills in place to support the agency, or not successfully completing one or more projects on time and within the allocated budget. Business risk is a consideration that should be included in the cost-benefit analysis.

Project risk. Project risk arises from several factors that inhibit system development projects from delivering a system that meets user expectations and that is delivered on time and within budget. Three factors that can be measured and used to determine the inherent degree of risk in a planned project are:

- project size -- resources as measured in worker time, calendar time, budget and dollar constraints, number of units affected, and geography.

- technology -- measured in terms of user and designer familiarity with and maturity of the technology used. The proposed new system may require technical functions that may not exist, or be in the research ("bleeding edge") phase (e.g., expecting a mainframe-based organization to develop a client-server system).

- system structure -- measured in terms of the precision used to define system objectives and output, the number and complexity of procedural changes that must be made in the agency to deploy the system, and the attitude and commitment of management, developers, and users of the system.

Understanding a project's risks can help the systems development manager choose the best design option for a given project and plan and control the project. Identification and discussion of areas of risk also enable users to become more informed decision-makers. Pinpointing risks during the earliest stages of project initiation increases the systems development staff's credibility and prevents unpleasant surprises later in the design and development effort. Consequently, the agency's top management should:

- ensure that the project team develops a risk management plan for mitigating risks associated with developing, acquiring, and operating the system;

- maintain continual oversight of the implementation of the risk management plan; and

- update the risk analysis and risk management plan in subsequent phases of the system life-cycle.

Audit Staffing Considerations

The audit steps discussed in all segments of this phase require a general understanding of IRM concepts, including how projects are scoped and system concepts developed. In those cases where a risk management plan has been developed by the agency, a technical specialist (information or computer/communication systems analyst familiar with systems risk assessment techniques) will be required to assess the significance of the risks and the agency's proposed mitigating techniques. Audits will require an information system analyst or ADP/telecommunication analyst to provide assessments of documents and qualifications of

the user and IRM team members. Where economic analyses, such as cost-benefit or return on investment need to be evaluated, an economist may be required.

The evaluator's knowledge base can be supplemented by attending one or more of the following GAO courses:

-- Introduction to Information Resources Management

-- Systems Development Life-Cycle Management

-- Information Systems Security

Additional Considerations

Auditors should view quality assurance (QA) as an indicator of the rigor applied by agencies in assessing performance. The goals of quality assurance are to help assess the quality of controls within the system and those controls surrounding the development of the system. QA ensures that systems (1) are developed in accordance with their stated objectives, (2) contain the needed internal controls and security to produce consistently reliable results, and (3) operate in conformance with IRM policies and procedures.

The effectiveness of the QA function should be determined to ascertain the degree of audit reliance that can be placed on it. This assessment generally encompasses quality, independence, professional proficiency, scope of work, performance of the audit work, and management of the internal audit department.

Agency Profile

The audit steps in this part rely on the agency profile for information on the IRM organization and applicable standards, policies, and procedures. System profiles will provide insight into the current IRM environment.

2.1.1 Project Initiation Segment

During this segment management approves a system development project and sets the stage for how the project will ultimately be designed and developed to address existing deficiencies and meet the agency's specific need or mission. In this segment, the project teams representing agency management, users, and IRM (system developers and managers) are put together to initiate the project. This team is expected to begin to document project-level planning activities such as budgeting, identifying problems with existing systems and/or processes, tasking, performance measures, methodology, and milestones. Typically, the project team is composed mostly of specialists from the agency's IRM office and all classes of users.

2.1.1.1 Agency Objectives for This Segment

2.1.1.1.1 Approve the initiation of a system development or modernization project.

2.1.1.1.2 Select the project teams with the appropriate skills necessary for successfully conducting the development or transition activities.

2.1.1.2 Relationship to Other Segments

During this segment the agency transitions from planning to actually developing a project identified in its Action Plan. It is during this segment that the agency pulls together the resources and capability needed to perform the segment tasks that follow.

2.1.1.3 Agency Products and Documents Delivered During This Segment

2.1.1.3.1 Authorization request and approval for the project.

2.1.1.3.2 Project teams charter that may include a mission statement, staffing levels, assignment of roles and responsibilities, and general approach for carrying out this phase of the project.

2.1.1.4 Management Responsibilities Discharged in This Segment

2.1.1.4.1 Authorize project initiation. Review and evaluate all project proposal planning documents and approve or reject proceeding with the project.

2.1.1.5 User Responsibilities Discharged in This Segment

2.1.1.5.1 Commit personnel to the project team who will ensure that the agency's primary purpose or mission (described as its business function) is fully considered and the proposed project will meet both existing and potential new user's needs as well as improve the agency's business function.

2.1.1.6 IRM Responsibilities Discharged in This Segment

2.1.1.6.1 Commit personnel to the project team who, with input from management and the users, will complete the remaining segments of this phase--that is, defining the project scope, developing the work plan, establishing the schedule, identifying (in general terms) what kinds of knowledge, skills, and abilities will be needed to complete the proposed project, and preparing a request for project approval by management.

2.1.1.7 Audit Objectives During This Segment

2.1.1.7.1 In this segment the auditor's objectives will be to determine whether (1) the project was approved by management, 2) the project team was staffed with the appropriate mix of skills and levels of expertise from the IRM and user organizations, and 3) whether the project addresses acknowledged deficiencies and systemic problems.

2.1.1.8 Audit Tasks for This Segment

2.1.1.8.1 Verify and document that management approval was obtained to initiate the project.

2.1.1.8.2 Determine that the project charter was developed and that it describes the project mission and objectives taking into account existing problems, establishes a project team and identifies the person in charge, and shows the specific responsibilities assigned to team members. Verify what the agency did to ensure that the team includes representatives from management, user, and IRM groups that will be affected by the project under development. Specific technical skills of team members should also be described. Evaluate whether the agency team has (1) a thorough understanding of the agency or department's information flow and method of operation, business area, and impediments, 2) produced a document that comprehensively

describes the business and system needs that are to be satisfied by the project, and (3) taken a realistic and business-oriented approach to satisfying the objectives of the project.

2.1.1.8.3 Evaluate the background and qualifications of project team members and make a judgment as to whether it was appropriate to assign them to the team. For example, on an Ada software development project it would not be appropriate to assign a software engineer who has no knowledge of the Ada programming language. Further, determine whether the appropriate staff with the necessary skills are represented on the project team. (Note: An information system or ADP/telecommunication analysts may be required to assess the qualifications of the team.)

2.1.1.9 Audit Products and Work Papers Developed in This Segment

2.1.1.9.1 Specific documentation should include, but not be limited to, management approval for project initiation, a copy of the project charter including the roles and responsibilities of project team members, and an analysis of the skills, abilities, and appropriateness of team members.

BLANK PAGE

2.1.2 Project Definition and Scope Segment

During this segment the project team defines the scope of the project and develops a system concept that is tied to the business area and business design to address existing deficiencies in legacy or problem systems. Scoping defines the project's boundaries--physical (platform, facility, and characteristics), functional (the activities the system is to perform), and budgetary (the amount of money available for developing the system), and barriers or impediments that constrain the implementation of the project or program. Scoping also begins the process of defining the technologies such as business and system architecture, security systems, integration issues such as electronic data interchange through interconnectivity and interoperability functions, telecommunications, data management and operating systems needed to develop the project. Once the project has been scoped, a total concept of operations (business plus systems) can be developed that describes the general approach for the project, its major components, and how they are intended to work together to meet the agency's mission. The system concept will eventually help drive project technical decisions such as hardware selection and software design. Finally, the project team develops information on the technical feasibility for the project and performs an analysis of the risks including costs and benefits that may hinder its success.

2.1.2.1 Agency Objectives for This Segment

2.1.2.1.1 Define the scope of the project within the confines and direction of the agency's business area analysis and business design. The scope will set the parameters for the project. The scope may range from an agency-wide project, or may just involve a particular sub-system within a division. Moreover, the scope may or may not involve acquiring entire new computing systems; for example, the addition of a new transaction or data management system for a financial management system may require transitioning legacy systems to newer databases, not computers.

2.1.2.1.2 Select a system architectural concept from alternative conceptual approaches. Architectural concepts may include centrally controlled or geographically distributed sites; be personal computer-based or use a combination of mainframe, mini- and microcomputers.

2.1.2.1.3 Select a transition or development approach model for implementing the solution system. Typically, three generic approaches are available for designing and implementing the solution system; these are 1) rapid prototype or iterative model, 2) the custom design approach, and 3) the commercial-off-the-shelf purchase followed by

integration. Often a mixture of one or more of these three approaches may be needed.

2.1.2.1.4 Estimate project initiation cost and the cost of the design phase.

2.1.2.1.5 Derive a rough order of magnitude life-cycle cost estimate using well-tested and industry accepted estimation techniques.

2.1.2.1.6 Perform a preliminary cost-benefit and risk analyses and develop information on technical feasibility using industry or federally recommended or internally tested methods.

2.1.2.1.7 Obtain management, user, and IRM concurrence on the proposed approach.

2.1.2.1.8 Identify project constraints.

2.1.2.2 Relationship to Other Segments

During this segment the project team will provide management with a general description of the project they are proposing to meet the agency's mission (or business function) and a rough order life-cycle cost estimate.

2.1.2.3 Agency Products and Documents Delivered During This Segment

2.1.2.3.1 Documentation on the deficiencies to be addressed and the scope of the project.

2.1.2.3.2 System concept developed from alternative approaches that were considered.

2.1.2.3.3 Preliminary cost-benefit analysis showing an economic analysis and design phase cost estimate including which functions generate the tangible estimated benefits, approximate one-time implementation costs, and approximate life-cycle costs.

2.1.2.3.4 Technical feasibility study.

2.1.2.3.5 Risk management analysis that includes:

a. Critical Success Factors: These would include essential or key issues, items, strategies, or people that if available or present lead to a high probability that a system or project will succeed in achieving its goal in a timely and cost-effective manner.

b. Contingency Options: These refer to scenarios of events and counter actions for abnormal situations such as the potential risks associated with fires and natural disasters, and malicious and inadvertent "break-ins" (electronic or manual) into the system facilities.

2.1.2.4 Management Responsibilities Discharged in This Segment

2.1.2.4.1 Ensure that all work done by the project team is validated by users.

2.1.2.4.2 Review project documents to ensure that the proposed project satisfies the need identified including deficiencies that must be ameliorated in the Action Plan.

2.1.2.5 User Responsibilities Discharged in This Segment

2.1.2.5.1 Review and validate the business operations, business area analysis, and concepts of operations as contained in the project definition segment. Validate the total concept of operations including the system concept.

2.1.2.5.2 Approve project scope and system concept including high-level requirements documents, request for proposal, and the initial test plan, if available.

2.1.2.6 IRM Responsibilities Discharged in This Segment

Provide support to the project team for:

2.1.2.6.1 Scoping the project in terms of business functions and system requirements.

2.1.2.6.2 Developing system concept based on alternative conceptual approaches closely tied to business needs. Include considerations for agency mission, business processes, safety, security, telecommunications, data and information management, operating

systems and platforms, architectures, and methodology to be used.

2.1.2.6.3 Preparing preliminary cost-benefit and risk management analysis, technical feasibility study, and initiation, design, and project life-cycle cost estimates.

2.1.2.6.4 Obtaining validation from managers and all classes of users for all documents generated in this segment.

2.1.2.7 Audit Objectives During This Segment

The auditor is concerned with determining whether (1) the project team has defined the scope of the project and developed an operational architecture and overall systems architecture based on an evaluation of existing deficiencies to be corrected. Ideally, several alternative conceptual approaches should have been analyzed; (2) preliminary cost and schedule estimates exist and whether these were developed using generally accepted models, and a rough order of magnitude life-cycle cost estimate; (3) preliminary cost-benefit, risk analyses, and technical feasibility studies exist; and (4) management, user, and IRM concur with the proposed approach.

2.1.2.8 Audit Tasks for This Segment

2.1.2.8.1 Determine whether the project team has scoped the project and developed a system concept that links to business objectives, will improve performance or service goals, and correct known deficiencies. Verify whether the system concept was selected after an evaluation of alternative conceptual approaches. Verify that users agree with the scope and system concept.

2.1.2.8.2 Obtain and evaluate all the cost and schedule related documents created in this segment. Determine whether the underlying assumptions, the life-cycle cost estimates, and the preliminary cost-benefit analyses are reasonable considering the uncertainty in the system design, organizational barriers, and impediments to change, and that estimated benefits are achievable. Expert opinion will be required to help with this analysis.

2.1.2.8.3 Determine if a technical feasibility study and a risk assessment exist. With assistance from a technical specialist assess the accuracy, completeness, and reasonableness of these documents. If any of these documents are unavailable, obtain the agency's rationale for this condition.

2.1.2.8.4 Determine whether agency management has monitored the progress and reviewed the documents developed in this segment. Verify that management and users understand the technical feasibility of the project and its associated risks. Finally, verify that management has approved the project's scope and system concept.

2.1.2.8.5 Determine that management has obligated sufficient funds to initiate the project and see it through to completion.

2.1.2.9 Audit Products and Work Papers Developed in This Segment

2.1.2.9.1 Copies of all pertinent documents that provide details on project scope, system concept (including the agency's analysis of alternative conceptual approaches), cost, risk, and technical feasibility.

2.1.2.9.2 Work papers summarizing (1) the information obtained by completing the audit plan and (2) the auditor's assessment of how well the agency has met the objectives of this segment.

2.1.3 Work Plan, Standards, and Project Organization Segment

In this segment the project team develops a detailed work plan, or road map, for monitoring and controlling the project. The plan usually includes a design and development schedule; project milestones; and a process for monitoring and reporting progress (including performance measures) for ensuring timely delivery and for providing effective resource and budgetary controls. During this segment the project team also reviews established policies and standards for security, system development methods, data integrity and reliability, acquisition models, and telecommunications and adopts those that should be used for the project (for example, protocols, security standards, software language, operating system, data dictionary, and computer-aided software engineering (CASE) tools). Finally, the project team proposes an organizational structure for completing the project.

2.1.3.1 Agency Objectives for This Segment

2.1.3.1.1 Develop the project work plan or work breakdown structure.

2.1.3.1.2 Establish appropriate controls for monitoring cost, schedule, and user satisfaction and for assessing whether the proposed system is likely to meet the agency's mission and program objectives.

2.1.3.1.3 Adopt existing standards and develop additional standards, if required, for the project.

2.1.3.1.4 Develop an organizational structure for completing the project.

2.1.3.2 Relationship to Other Segments

This segment sets the stage for proceeding to the design phase. The work plan, standards, and organizational structure provide the framework necessary to begin designing and developing the project.

2.1.3.3 Agency Products and Documents Delivered During This Segment

2.1.3.3.1 Work plan.

2.1.3.3.2 Project standards.

2.1.3.3.3 Organizational structure.

2.1.3.4 Management Responsibilities Discharged in This Segment

2.1.3.4.1 Ensure user and IRM coordination.

2.1.3.4.2 Review and approve the work plan, project standards, and organizational structure.

2.1.3.5 User Responsibilities Discharged in This Segment

2.1.3.5.1 Work with the project team to identify and commit personnel with the necessary skills for designing and developing the project.

2.1.3.5.2 Review the work plan, project standards, and organizational structure developed by IRM. Provide feedback to the project management team and management on their reasonableness.

2.1.3.6 IRM Responsibilities Discharged in This Segment

Provide support to the project team for:

2.1.3.6.1 Developing the work plan.

2.1.3.6.2 Adopting a set of standards for designing and implementing the system, risk management, security, telecommunications, data structures, federal compliance requirements to open systems architectures, and configuration management for the project.

2.1.3.6.3 Selecting project management tools for the development environment and for monitoring the project.

2.1.3.6.4 Defining the organizational structure, that is, the components within the agency that will be involved in the project; identifying a project leader; and defining project resource requirements.

2.1.3.6.5 Obtaining user agreement on the work plan, project standards, and organizational structure and commitment for proceeding into the design phase.

2.1.3.7 Audit Objectives During This Segment

The auditor should identify whether:

2.1.3.7.1 the project team developed a reasonable work plan and controls for monitoring the project in conformance with agency directives, adopted standards for security, data structures, telecommunications, and open systems compatibility, and established an organizational structure to monitor, build, test, operate and maintain the system,

2.1.3.7.2 the user reviewed and agrees with the project team's proposals, and

2.1.3.7.3 management reviewed and approved the documents developed in this segment ensuring that risks and system vulnerabilities were identified and a plan to minimize these was developed, and that agency directives and federal acquisition standards were followed.

2.1.3.8 Audit Tasks for This Segment

2.1.3.8.1 Verify that a work plan and controls for monitoring the project were established. Make a judgment as to whether the schedule, milestones, and monitoring and controlling process are reasonable.

2.1.3.8.2 Assess whether standards have been adopted for the project. Independently verify that the adopted standards are consistent with generally accepted standards and practices used within the agency. Expert opinion may be required to perform the analysis.

2.1.3.8.3 Verify that the project team developed an organizational structure for the project. Verify that the structure identifies the departments within the agency that will be involved in the project, the person responsible for completing the project's design, and the kind of resources that will be needed to complete the project.

2.1.3.8.4 Determine whether users have reviewed the work plan and adopted standards and an organizational structure for designing the project and agree with them.

2.1.3.8.5 Interview management and obtain verification that they have reviewed and approved the documents developed in this segment and agree with the approach proposed by the project team.

2.1.3.9 Audit Products and Work Papers Developed in This Segment

2.1.3.9.1 Copies of all pertinent documents that provide details on the work plan, adopted standards, and the organizational structure for completing the project scope.

2.1.3.9.2 Work papers summarizing (1) the information obtained by completing the audit plan and (2) the auditor's assessment of how well the agency has met the objectives of this segment.

2.1.4 Management Review and Approval Segment

Management (1) reviews all the documents developed in this phase to determine whether the proposed project will correct known deficiencies, satisfy the user's needs, and achieve the agency's goals; (2) makes a judgment as to whether the system is feasible within budget constraints, technologically feasible, and can be completed with acceptable risk of cost and schedule failures; and (3) approves the project to proceed to the design and development phase.

2.1.4.1 Agency Objectives for This Segment

2.1.4.1.1 Ensure that the proposed project will correct existing deficiencies in legacy information systems. Additionally, if improved service and performance goals have been set, then management must ensure that these goals can be met with a reasonable chance of success.

2.1.4.1.2 Ensure that the user and IRM organizations agree with the project team's proposal.

2.1.4.1.3 Obtain management approval of the products and proposal developed in this phase and its authorization to begin the design and development phase.

2.1.4.2 Relationship to Other Segments

2.1.4.2.1 This is the final segment of the Concept and Project Initiation Phase. Successful completion of this segment moves the project to the design and development phase.

2.1.4.3 Agency Products and Documents Delivered During This Segment

2.1.4.3.1 A project team report that details the project's scope, the system concept, the work plan, adopted standards, and the organization structure for completing the project. The report also includes economic and technical analyses such as cost-benefit, feasibility, technical alternatives, and risk analyses.

2.1.4.3.2 Management's approval to proceed with the design and development phase.

2.1.4.4 Management Responsibilities Discharged in This Segment

2.1.4.4.1 Review the project team report. Ensure that the proposed system and business operations will improve service or performance goals.

2.1.4.4.2 Authorize proceeding with the design and development phase, if appropriate.

2.1.4.5 User Responsibilities Discharged in This Segment

2.1.4.5.1 Collaborate with the project team in preparing the report and obtaining project approval from management.

2.1.4.6 IRM Responsibilities Discharged in This Segment

Provide support to the project team for:

2.1.4.6.1 Preparing the report and obtaining user's concurrence.

2.1.4.6.2 Submitting the report to management for approval.

2.1.4.7 Audit Objectives During This Segment

2.1.4.7.1 The auditor should assess whether agency management has reviewed the project team's report and approved the proposed project to proceed to the design and development phase.

2.1.4.8 Audit Tasks for This Segment

2.1.4.8.1 Determine whether the project team completed and submitted its report (or similar documentation) to agency management for review and approval. Verify that the user and IRM organizations reviewed the project team's report and agreed with its contents.

2.1.4.8.2 Determine whether management reviewed the project team's report, approved the project, and authorized the project team to proceed to the design and development phase. Document this action.

2.1.4.9 Audit Products and Work Papers Developed in This Segment

2.1.4.9.1 Copies of the project team report and evidence of management's approval of the project and authorization to proceed.

2.1.4.9.2 Work papers summarizing (1) the information obtained by completing the audit plan and (2) the auditor's assessment of how well the agency has met the objectives of this phase.

BLANK PAGE

Contents of the Design, Development, and Deployment Phase

3.0 The System Design, Development, and Deployment Phase

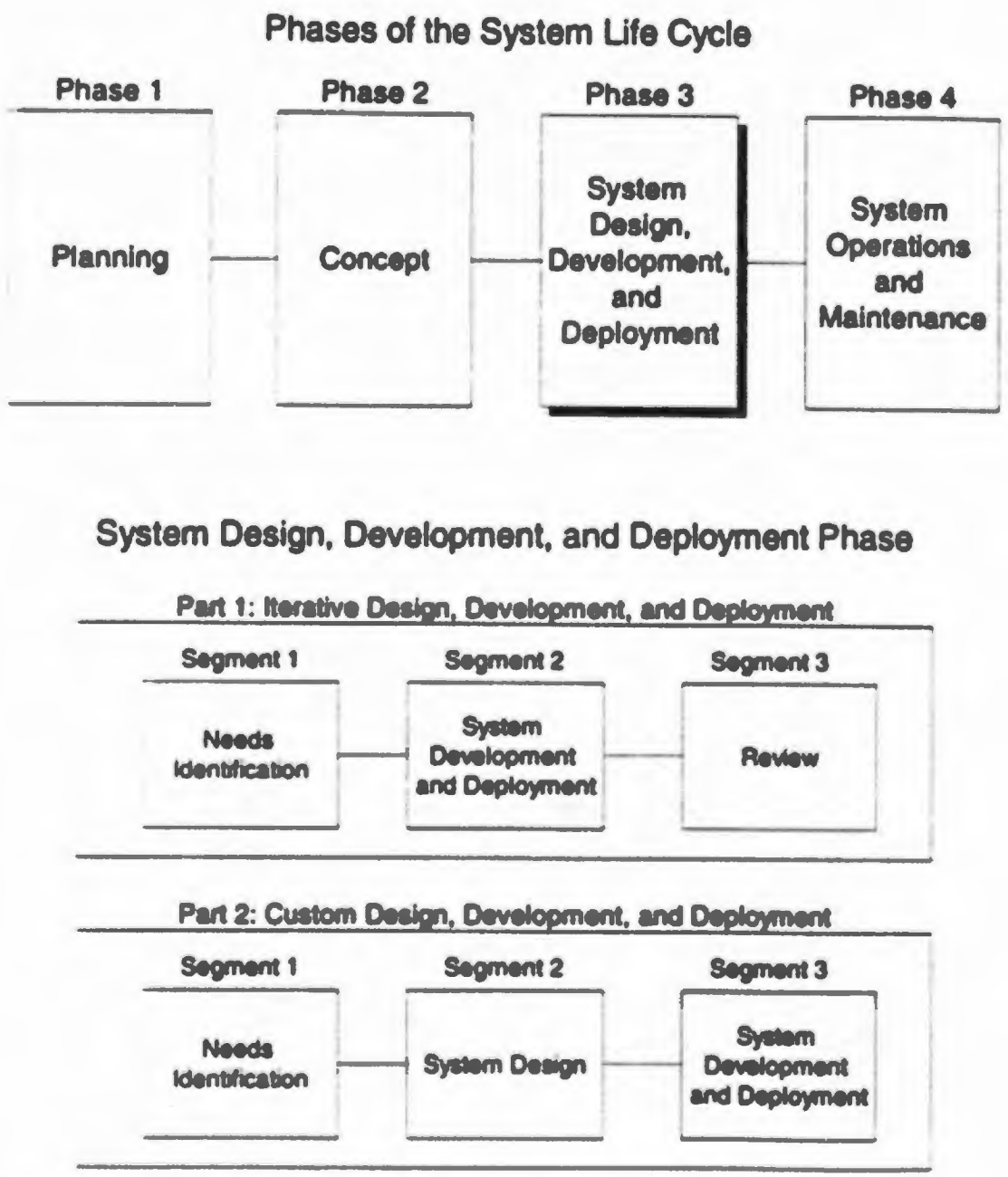

Figure 5. The System Design, Development, and Deployment Phase

The purpose of this phase is to (1) define the detailed functional and technical specifications for the system in as complete a manner as possible; (2) design the system in accordance with the detailed specifications, considering the expected operating environment; (3) develop (i.e., code, integrate, and test) the system using one or more development techniques (i.e., waterfall, spiral, evolutionary); (4) evaluate the quality of the system using quality assurance (e.g., peer reviews, structured walkthroughs, in-process reviews) and quality control (e.g., critical design review, functional qualification test, independent verification and validation (IV&V)) techniques; (5) obtain user acceptance of the system; (6) deploy the system in accord with an approved set of detailed plans (i.e., transition, deployment, and operations plans); and (7) define the management actions necessary for controlling risks and improving the likelihood of a successful system. The completion of this phase establishes the operational baseline for the next phase which is the operations and maintenance phase.

This phase is presented as two parts, each representing a particular method for designing and developing automated systems. The first part is designated as "iterative design, development, and deployment" and the second part is called "custom design, development, and deployment." The iterative method recognizes the reality of vague or incomplete functional requirements and specifications; thus it contains many risk reduction techniques such as rapid prototyping, spiral mode and or evolutionary model. The custom method tends to follow the traditional waterfall method whereby it is assumed that most functional requirements and specifications can be defined prior to detailed system design and development. Prior GAO and IG reports have shown this method be more risky than the iterative method. However, the two methods do not have to be mutually exclusive.

The custom approach does not have to use the traditional waterfall method as described above. The iterative approach can be used to design and develop customized systems. Such an approach will allow for multiple working prototypes, as well as feedback to both the requirements determination process and the system design. Additionally, a software package or set of packages procured from the commercial marketplace (i.e., often referred to as commercial-off-the-shelf (COTS) software) can be customized using either the traditional waterfall method or the iterative method.

If used, COTS items must be integrated into the overall design of the system. They should not be modified unless it is an absolute necessity. Prior to any modifications, management should be apprised of the potential operations and maintenance consequences (i.e., loss of supplier maintenance support, inability to keep up with new releases of the product, more human resources to maintain the product) of any modifications. If COTS products are to be used in a stand-alone mode or as a supplement to another system then interface requirements must be identified and defined as well as the details associated with transition, deployment, and operations. Placing COTS products into operations should follow a method similar to the final stages (i.e., initial operational capability (IOC), transition, and deployment) of the custom design method.

3.1 Iterative Design, Development, and Deployment

The iterative method is generally used when the agency wants to develop a system while minimizing the risks associated with developing systems that have either ambiguous or incomplete requirements or are using immature or untested technology. In SAF, iterative refers to a set of techniques that include: (1) prototyping (i.e., engineering breadboarding or rapid prototyping) and (2) evolutionary (i.e., spiral model).

Prototyping is an effective paradigm for reducing risks in system engineering (i.e., hardware and software) efforts. It can serve as a mechanism for defining requirements. After requirements definition, the prototype can be discarded (at least in part) and the actual hardware, firmware, or software can be engineered with a focus on quality.

The evolutionary technique enables the design and development team and the users to understand and react to risks at each evolutionary level. It uses prototyping as a risk reduction mechanism at any stage in the evolution of the product. It maintains the systematic approach of the traditional AIS life-cycle (i.e., waterfall method), but incorporates it into an iterative framework that more realistically reflects the real world.[1] A piece of the system is built, tested, and installed then another piece is built, tested and installed, and so on. The number of iterations is unknown. Therefore, an attempt to predict overall development or life-cycle costs at the design stage is risky. Similarly, product schedule forecast will also have a high degree of uncertainty at the design stage.

The advantage of this approach is that useable products can emerge at an earlier phase than is possible using the traditional AIS waterfall approach. The payoff here is in lowered potential for system redesign which reduces costs associated with making changes in the later phases. Planning, project definition, requirements analysis, system development, and testing are typically done almost concurrently with feedback from users or the system tests occurring on a day-to-day basis.

Open communications and close interaction between small groups of users and developers are characteristics of this approach. These characteristics minimize the number of communication channels to be established and maintained and create an environment in which user-driven change requirements can be implemented with a minimal top-down design effort needed.

The iterative approach is sometimes incorporated into the traditional AIS life-cycle (i.e., waterfall or grand design methods) of the custom design and development method when user operational requirements and functional specifications cannot be developed "a priori." In this case, iterative methods bring a more realistic approach to the determination of operational requirements and expected functions and features of the system. The iterative method can be used as an experimental "learn-as-you-go" approach.

---

[1] Roger S Pressman, Software Engineering : A Practitioner's Approach, McGraw-Hill,Inc., 1992.

Developing a system under any of the iterative approaches involves the following three segments:

-- Needs Identification and Design: Determine which iterative approach the agency will use, design the work plan, and identify the technical documents needed for building the deliverables.

-- System Development and Deployment (Code, Test and Deploy): Using the iterative method, develop sections of code in small, manageable increments; design test plans; and conduct tests. Complete development of the system by repeatedly coding and testing the system. Finally, conduct user tests of each increment at sites (i.e., alpha and beta test sites) that are representative of the entire user environment. Continue until all required increments are completed.

-- Review: Management, users, and IRM staff review the system and decide (a) whether the upgraded or new system meets the agency's needs; or (b) whether additional enhancements or a new system are still necessary; or (c) whether the project should be abandoned.

Risk Management

The management of risk is a key part of the iterative approach. As such, the agency should identify and develop a plan that addresses project management and technical risks such as availability of skilled personnel, accuracy of cost projections and schedule estimates, system complexity, use of newly emerging technologies, and so on. Specific issues that may be considered include:

-- determining whether the iterative method needs to be used exclusively or in combination with either the custom or packaged methods;

-- establishing a software engineering environment (i.e., Computer-Aided Software Engineering (CASE) tools) that facilitates the iterative approach;

-- understanding the experimental nature of the iterative approach (i.e., even though a system may fail because it does not meet user needs, the experience may provide beneficial knowledge through lessons learned);

-- understanding that there are no precise methods for predicting the number of iterative cycles and the costs associated with these cycles;

-- understanding that this approach must deal with continual changes in scope and user requirements between successive iterations; and

-- identifying and mitigating threats to the security of the proposed system.

A risk management plan should ensure that none of the following shortcomings will affect the project: [4]

-- unjustified or never-ending prototyping projects;

-- insufficient documentation developed for a prototype subsequently used in an interim production environment;

-- unclear prototype objectives;

-- prototyping used to avoid documentation or controls;

-- poor definition of the responsibilities between data processing and the user organization;

-- lack of proper tools or training on the use of the tools;

-- lack of proper consideration of agency-wide information and data requirements;

-- undefined performance measures.

Audit Staffing Considerations

The audit steps discussed in all segments of this phase require, as a minimum, a general understanding of the agency's business and IRM concepts. Experience in system development, particularly in the use of iterative methods, would be a valuable asset to the audit. Computer/telecommunications and information system analysts with knowledge and work experience in software engineering will be required to evaluate or assess the processes and status in this segment.

The evaluator's knowledge base can be supplemented by intensive training in software engineering for project management, structured systems analysis and design, and structured programming techniques. More basic supplemental training would include GAO or external courses in one or more of the following areas:

-- Introduction to information resources management

---

[4] Spectrum International Inc., Brochure titled "SPECTRUM/Prototyping - The Stand-Alone Prototyping Methodology", 2600 Boyce Plaza Road, Pittsburgh, PA. 15241.

- Systems development life-cycle management
- Information systems security
- System maintenance
- System analysis

Additional Considerations

If the agency has a QA function, it should obtain concurrence from QA on the project's technical and economic feasibility. It should also ensure that the approach used for developing the proposed new system is valid for this and subsequent segments. The agency can also benefit from the use of an internal audit function for reviewing internal controls in this phase.

Agency Profile

This part relies on the agency profile for information regarding the current IRM organization and standards, policies, and procedures. Past reviews, audits, or studies may direct the audit team to deficiencies in the system development process. System profiles provide insight into the current IRM environment.

3.1.1 Needs Identification and Design Segment

In this segment, the agency identifies specific user requirements and selects the iterative approach (i.e., prototype or spiral) that will be used for designing, developing, and testing the system. Additionally, the agency (1) reviews and updates the cost and schedule; (2) develops policies and procedures for transitioning to the proposed system, and (3) submits a proposal requesting management's approval to proceed.

3.1.1.1 Agency Objectives for This Segment

3.1.1.1.1 Identify specific user needs, including requirements for performance, security, reliability, testing, and data integrity controls.

3.1.1.1.2 Define what will be delivered (e.g., user screens, database reports, graphics).

3.1.1.1.3 If contractual support is needed to assist with the identification of requirements, design, and development, then prepare, review, and release a request for proposal (RFP) for competitive bids.

3.1.1.1.4 Ensure an environment that facilitates on-going communication between users and developers. The use of regular technical interchange meetings is a means for facilitating open communications.

3.1.1.1.5 If the proposed solution is being designed for a legacy system (existing data base) or an existing prototype, the project team describes and documents the existing system's input, output, and processing functions in order to correct deficiencies or make enhancements.

3.1.1.1.6 Determine and define the iterative approach to be taken for implementing the proposed system to meet the agency's business needs.

3.1.1.1.7 Examine system architectural alternatives that have a high potential for satisfying the user's needs.

3.1.1.1.8 Develop a work plan that explicitly identifies the resources required. For significant levels of effort, identify the criteria for starting and ending each activity related to specific segments of work.

3.1.1.1.9 Establish appropriate computing resources (i.e., program development workbench and software support tools).

3.1.1.1.10 Review issues such as (1) system architecture and major components of the system (i.e., telecommunications, operating system, database management systems, user and system interfaces, security) and their interrelationships; (2) the function of each component; (3) data and information architecture; (4) system performance requirements; (5) political or organizational dynamics between potential users and service providers and their impact on the project; (6) quality assurance and control processes; (7) system configuration management; and (8) training.

3.1.1.1.11 Develop test plans and set up an independent testing agent, if necessary (i.e., for medium to large systems).

3.1.1.1.12 Prepare estimated project costs using either parametric cost estimating models or heuristic models using a consensus of experience. There are several commercially available software cost estimating models such as the Constructive Cost Model (COCOMO) and the Software Life Cycle Management (SLIM) model. Prepare estimated schedules using either commercially available software packages or customized in-house techniques.

3.1.1.1.13 If a risk management plan already exists, review and update the risk analysis to properly address issues such as (1) AIS security and safety considerations; (2) system performance; (3) staffing and skills needed; (4) training; (5) cost and schedule exposure; (6) technical viability; and (7) impact of the new system on the organization. If a risk management plan does not exist then such a plan needs to be developed.

3.1.1.1.14 Verify and validate all analyses and plans that are developed. Resolve open issues regarding major technical and interface requirements.

3.1.1.1.15 Develop and review the proposed conversion or reengineering plans.

3.1.1.1.16 Develop and review policies and procedures that support the transition to the new system.

3.1.1.1.17 Obtain management approval for the deliverables from this segment

3.1.1.2 Relationship to Other Segments

This segment starts with the output of the Concept and Project Initiation phase for the purpose of enhancing an existing system or developing a new one. The products and documents developed in this segment lay the foundation for the system development and installation segment that follows.

3.1.1.3 Agency Products and Documents Delivered During This Segment

Documents and products may have different names in the agencies. No matter what they are called, these documents and products should provide the following information:

- 3.1.1.3.1 high-level user requirements describing the general nature of the problem to be solved or the enhancement that is needed;
- 3.1.1.3.2 overview of the current system, including a description of the architectural and operational features that are linked to acknowledged system deficiencies;
- 3.1.1.3.3 system functional requirements (translation of user requirements into specific system functions, such as screen displays, report formats, network requirements);
- 3.1.1.3.4 work plan (schedule, activities, personnel);
- 3.1.1.3.5 description of alternative technical solutions (see GAO/IMTEC-92-51 for an example of alternatives analysis);
- 3.1.1.3.6 updated cost-benefit analyses;
- 3.1.1.3.7 updated risk analyses for cost and schedule failure, and interconnectivity and interoperability, including security requirements;
- 3.1.1.3.8 design of quality control and assurance and configuration management processes;
- 3.1.1.3.9 project status reports;
- 3.1.1.3.10 records of meetings with users and management;
- 3.1.1.3.11 project request document approving this and subsequent segments;
- 3.1.1.3.12 RFP, if appropriate.

3.1.1.4 Management Responsibilities Discharged in This Segment

3.1.1.4.1 Approve the scope of the iteration being identified and developed.

3.1.1.4.2 If contractual support is needed, (1) approve the solicitation document (e.g., RFP or IFB) and (2) forward an Agency Procurement Request (APR) to the GSA to obtain a delegation of procurement authority (DPA), if required.

3.1.1.4.3 Review cost and risk analyses.

3.1.1.4.4 Require that IRM and user organizations work together to ensure that the iteration being developed meets user needs.

3.1.1.4.5 Ensure that the required computing resources (including software support tools) are available.

3.1.1.4.6 Review the products and deliverables.

3.1.1.4.7 Authorize proceeding with this iteration.

3.1.1.4.8 Monitor the project's progress using the defined quality control and assurance process.

3.1.1.5 User Responsibilities Discharged in This Segment

3.1.1.5.1 Identify and define requirements.

3.1.1.5.2 Specify performance, security, and integrity requirements.

3.1.1.5.3 Ensure that personnel with appropriate business and functional skills are available to execute this phase.

3.1.1.5.4 Participate with appropriate IRM staff to select a particular iterative method.

3.1.1.5.5 Participate with the appropriate IRM staff to design and document the system.

3.1.1.5.6 Work with the IRM staff to update the economic and technical alternative analyses.

3.1.1.5.7 Verify and validate system requirements.

3.1.1.6 IRM Responsibilities Discharged in This Segment

3.1.1.6.1 With user participation, develop (1) system functional requirements; (2) system specifications including database specifications; (3) updated technical alternative approaches to satisfy user needs; (4) an economic analysis; and (5) a risk analysis.

3.1.1.6.2 With user assistance, choose the iteration method and develop the overall iteration approach.

3.1.1.6.3 Ensure that policies and procedures are established for transitioning to the new system with minimal disruption to current business operations.

3.1.1.6.4 Participate with the appropriate user staff to design and document the system.

3.1.1.6.5 With user coordination, prepare design specifications for internal controls, data reliability and integrity, and system performance.

3.1.1.6.6 Prepare and present to management a request for approval to proceed with development.

3.1.1.6.7 Prepare and present progress reports to management.

3.1.1.6.8 Prepare and advertise the RFP or similar solicitation document, if appropriate.

3.1.1.6.9 Implement the quality assurance and control plan. Develop and implement a configuration management process.

3.1.1.7 Audit Objectives During This Segment

3.1.1.7.1 Determine whether the user and functional requirements are adequately defined and validated. Also determine if these requirements have been translated into design specifications through a structured process that included a rigorous quality assurance and control discipline.

3.1.1.7.2 Determine whether the agency has established a development team involving users and IRM staff with the appropriate skills.

3.1.1.7.3 Determine whether the agency has allocated the appropriate computing resources for this project.

3.1.1.7.4 Determine if the agency has identified risks inherent in the iterative approach selected, and developed a management plan for mitigating these risks.

3.1.1.8 Audit Tasks for This Segment

3.1.1.8.1 Identify projects that haven't yielded a completed product (i.e., a working set of computer programs or an information product such as a report).

3.1.1.8.2 Identify unrealistic costs and schedules that were estimated using ad hoc methods. Verification of costs and schedules may be required using formal tools such as COCOMO or SLIM.

3.1.1.8.3 Determine whether sufficient documentation was developed for a prototype that was subsequently used in an interim production environment.

3.1.1.8.4 Identify ambiguous prototype objectives. Determine if the prototype was approved by management.

3.1.1.8.5 Identify a vague delineation/definition of the responsibilities between the IRM organization and the user organization.

3.1.1.8.6 Determine whether the agency performed a business area analysis prior to choosing a particular design model.

3.1.1.8.7 Review the agency's rationale for selecting the iterative approach. The rational should be based on risk aversion.

3.1.1.8.8 Review the agency's technical alternatives analysis. If the analysis is deficient in one or more of the following areas, then the deficiencies should be regarded as potential findings:

a. incomplete;
b. vague;
c. not traceable to agency mission or goals;
d. unduly restricted options considered;
e. automates existing processes without considering improvements in product or service quality; and
f. not supportable (i.e., makes unsubstantiated claims).

3.1.1.8.9 Obtain and review the agency's documentation and analyses that demonstrate that the design specification is consistent with the functional and operational requirements.

3.1.1.8.10 Verify that the agency has a risk management plan that identifies risks associated with personnel, cost, schedule, technology and any other unique features that could jeopardize the project's success.

3.1.1.8.11 Verify that the project management team consistently applied accepted standards and criteria for system design.

3.1.1.8.12 Determine whether the appropriate number of staff, personnel skills, training, tools, and computing resources are available to the project team.

3.1.1.8.13 Obtain and review documentation (e.g., conversion or reengineering plan) describing how the agency will transition to the new system with minimal disruption.

3.1.1.8.14 Evaluate the RFP or similar solicitation documents for anomalies, inconsistencies, and restrictiveness.

3.1.1.8.15 Verify that the agency's quality assurance and control functions have been exercised appropriately in this segment.

3.1.1.9 Audit Products and Work Papers Developed in This Segment

Work papers summarizing the auditor's analysis should include:

3.1.1.9.1 an analysis of agency documents developed in this segment for completeness, consistency, and traceability to the accepted concept of operation;

3.1.1.9.2 an evaluation of the economic analysis and technical alternative products produced by the agency;

3.1.1.9.3 an analysis of the agency's risk management plan for mitigating project risks; and

3.1.1.9.4 an analysis of the proposed conversion or reengineering approach.

BLANK PAGE

3.1.2 System Development and Deployment Segment

The focus of the development and deployment segment is on implementing the detail design and on writing code for the system. System development is completed by iteratively building and testing sections of code, and then using test results to further refine the software. The agency selects the hardware, retests the software on it, and finally installs the completed system. This occurs, hopefully, with minimal disruption to users and the existing system.

3.1.2.1 Agency Objectives for This Segment

3.1.2.1.1 Reconfirm requirements for users and for such features as performance, security, and integrity controls.

3.1.2.1.2 Complete the detailed design, if necessary.

3.1.2.1.3 Develop the code (processing logic) and the test plans using structured system design and programming techniques.

3.1.2.1.4 Revise the initial estimates for cost, schedule, level of effort, and computing resource requirements.

3.1.2.1.5 Ensure that all interfaces have been identified (i.e., system to system interfaces, system to human interfaces).

3.1.2.1.6 Reevaluate the technical alternatives to ensure that they still satisfy the user's functional and operational requirements.

3.1.2.1.7 Continue to reiterate design, coding, and testing until users are satisfied and accept the system.

3.1.2.1.8 Obtain management approval that the system satisfies user requirements and meets the agency's mission needs.

3.1.2.1.9 Install the system at an initial operational site. This is sometimes referred to as the initial operational capability (IOC). If the system is required by multiple sites, then a deployment plan and strategy will be required.

3.1.2.1.10 Update and review risk analyses.

3.1.2.2 Relationship to Other Segments

This is the second segment in the iterative design, development, and deployment part. Building on outputs from the needs identification and design segment, the agency completes the detail design and begins building the system, prototype, retest, and so on. The products developed in this segment form the basis for determining whether enhancements or a new system will be necessary.

3.1.2.3 Agency Products and Documents Delivered During This Segment

The agency documents and products should typically provide the following information:

3.1.2.3.1 completed system or subsystem;

3.1.2.3.2 detailed design document;

3.1.2.3.3 program documentation and code listings for application programs and database conversion (if appropriate);

3.1.2.3.4 evidence of verification and validation of test plans and test results;

3.1.2.3.5 integration charts or diagrams, where appropriate, for systems not designed as stand-alone systems.

3.1.2.3.6 evidence that management and IRM staff have performed "walk-through" to approve design and code;

3.1.2.3.7 evidence of user and management acceptance;

3.1.2.3.8 records of change requests;

3.1.2.3.9 updated work plan (schedule, activities, personnel);

3.1.2.3.10 updated economic analysis and risk analyses;

3.1.2.3.11 project status reports;

3.1.2.3.12 records of meetings;

3.1.2.3.13 request for management approval of all design iterations;

3.1.2.3.14 RFP or other solicitation document, if appropriate.

3.1.2.4 Management Responsibilities Discharged in This Segment

3.1.2.4.1 Reconfirm scope of the project.

3.1.2.4.2 Ensure that IRM and user organizations coordinate on test results and system changes.

3.1.2.4.3 Ensure that the products from this segment meet the agency's mission and satisfy user requirements.

3.1.2.4.4 Monitor progress of the project.

3.1.2.5 User Responsibilities Discharged in This Segment

3.1.2.5.1 Reconfirm user requirements, as well as requirements for performance, security and integrity, and ensure that such requirements are met.

3.1.2.5.2 Ensure that the system and its documentation satisfies user needs.

3.1.2.5.3 Work with the IRM organization to update economic and technical alternatives.

3.1.2.5.4 Identify and inform management of changes to the user organization that may result from using the system.

3.1.2.6 IRM Responsibilities Discharged in This Segment

3.1.2.6.1 Create and update all technical documentation such as high-level system designs, detailed system and sub-system designs, software documentation, technical reference manuals, training manuals, user procedures and so on.

3.1.2.6.2 Incrementally and iteratively develop code, test, and install the proposed system, recognizing that the system may change due to changes in user operational and functional requirements.

3.1.2.6.3 Review and update technical alternative approaches to satisfy user needs.

3.1.2.6.4 Update economic and risk analyses.

3.1.2.6.5 Update established procedures for manual and automated processes.

3.1.2.6.6 Prepare and present progress reports to management.

3.1.2.7 Audit Objectives During This Segment

3.1.2.7.1 Determine whether the agency has adequately addressed risks as the project proceeds through this segment.

3.1.2.7.2 Determine if the development and installation objectives have been met.

3.1.2.8 Audit Tasks for This Segment

3.1.2.8.1 Review the agency's documentation to determine whether the detailed designs, code, and test results are completely documented.

3.1.2.8.2 Determine if cost and schedule estimates, resource requirements, and performance specifications have been updated and documented.

3.1.2.8.3 Review the thoroughness of the agency's validation and verification process, and verify with the user organization whether the system satisfies the functional and operational requirements of the users (i.e., Are 90 percent of all prescription orders filled at army hospital "X" completed in 10 minutes or less?) If not, why not?

3.1.2.8.4 Review the updated risk analyses and assess whether the agency's analysis is reasonable.

3.1.2.8.5 Verify that the project management team consistently applied accepted standards and criteria in building the system.

3.1.2.8.6 Evaluate whether appropriate skills and resources were available and used in this segment.

3.1.2.8.7 Obtain and evaluate the RFP or similar solicitation documents for (1) completeness; (2) traceability to agency concept of operations and mission goals; and (3) consistency.

3.1.2.8.8 Determine whether the agency used the experience it gained in iteratively developing the system to improve or change its operations (i.e., lessons learned).

3.1.2.8.9 Determine whether agency policies and procedures were followed for installing the system and whether the installation occurred with minimal disruption to the user and normal business operations.

3.1.2.8.10 Verify with management that the installed system is meeting the agency's mission needs.

3.1.2.8.11 Ensure that management approved moving into the next segment.

3.1.2.9 Audit Products and Work Papers Developed in This Segment

Work papers should summarize facts and potential findings for the following agency documents and actions:

3.1.2.9.1 the agency's risk management plan and process;

3.1.2.9.2 the transition plan for conversion and cutover from the legacy environment (i.e., process and system) to the replacement environment;

3.1.2.9.3 the economic analysis and the technical alternatives analyses, including an evaluation of the derivation of the economic estimates and the assumptions behind the technical alternatives;

3.1.2.9.4 adherence to system and software engineering principles and practices.

BLANK PAGE

3.1.3 Review Segment

Once the system is developed, management, users, and IRM staff review it and decide whether it meets the agency's needs or whether additional enhancements or a new system may be necessary. The focus of this segment is either on accepting the system as operational, abandoning it, or continuing to refine the system through lessons learned in the development and installation process. Should the development team identify needed enhancements or revisions to the development strategy, it obtains management approval and resources to continue to iterate, abandon the project, or go back to the planning phase.

3.1.3.1 Agency Objectives for This Segment

3.1.3.1.1 Review the results of a formal operational test and evaluation conducted by a team independent of the project team that developed the AIS. If the results are positive, proceed to the operations and maintenance phase.

3.1.3.1.2 If the system does not satisfy user needs, decide whether to continue developing the system using the same iterative approach (next cycle), a new strategy, or abandon the system.

3.1.3.1.3 Review and compare cost and schedule estimates to actual expenditures for this segment.

3.1.3.1.4 Ensure that communication channels to users remain open.

3.1.3.1.5 If external vendor support is still needed for further development, then review and approve the RFP or other solicitation request.

3.1.3.2 Relationship to Other Segments

This segment determines if the project team has produced a system or portion thereof that is suitable for installation at a single user site or wide-scale deployment to multiple sites. If a user site is chosen as an alpha site, this is usually for experimentation with the end product in a real world environment for the purpose of refining the functions, features, and operational characteristics (i.e., response time, availability, reliability) of the system. Occasionally, agencies may use the concept of a beta site to test the suitability of the system for wide-scale deployment. This normally involves choosing a set of real world sites that represent a subset of the sites designated for deployment. The working assumption is that the subset of sites is representative in terms of their operational characteristics of the universe of designated deployment sites.

3.1.3.3 Agency Products and Documents Delivered During This Segment

The agency's documents and products should typically provide the following information:

3.1.3.3.1 a summary and analysis of experience gained in this segment;

3.1.3.3.2 records of user acceptance and a decision to proceed to the operations and maintenance phase or evidence of additional enhancements and a decision to continue reiterating; or evidence of a decision to abandon the project, and

3.1.3.3.3 RFP (if appropriate)

3.1.3.4 Management Responsibilities Discharged in This Segment

3.1.3.4.1 Based on the results of the final risk analysis performed in the preceding segment, review the status and results of the development effort and decide whether to accept the system as operational, abandon it, or continue with development.

3.1.3.4.2 Reconfirm that IRM and user organizations are effectively coordinating on key aspects of the development effort (i.e., minutes of meetings, user acceptance test signoffs).

3.1.3.4.3 Provides the funding and resources for the selected iterative method and approves the proposed schedule.

3.1.3.4.4 If management decides to stop the project, then authorize abandoning the project.

3.1.3.5 User Responsibilities Discharged in This Segment

3.1.3.5.1 Decide whether the entire system or part of the system meets their requirements.

3.1.3.5.2 Decide whether to proceed with subsequent iterative cycles to more closely meet their actual functional and operational requirements.

3.1.3.6 IRM Responsibilities Discharged in This Segment

3.1.3.6.1 Confirm that completed iterations meet user requirements.

3.1.3.6.2 Continue to prepare and present progress reports to management.

3.1.3.6.3 If development is to continue, work with users to refine system functions, features, and operational characteristics.

3.1.3.6.4 Define and document "lessons learned" from the already implemented and installed iterative cycle(s).

3.1.3.6.5 Complete all relevant system documentation for the AIS to be installed.

3.1.3.7 Audit Objectives During This Segment

3.1.3.7.1 Determine if management has provided sufficient oversight over the project.

3.1.3.7.2 Determine whether the agency has adequately addressed risks in proceeding to additional iterations.

3.1.3.8 Audit Tasks for This Segment

3.1.3.8.1 If the project has not been abandoned, review updated cost and schedule and determine whether expended resources have been recorded properly and warrant proceeding with the project.

3.1.3.8.2 Determine whether the risk analyses provide a sound basis for continuing or abandoning the project and check this against the agency's decisions.

3.1.3.8.3 Verify that the agency has (1) developed a system that meets user functional and operational requirements including performance expectations; (2) formally approved the system to transition to operational status; (3) documented the need for additional enhancements and approved continuing development iterations; or (4) documented its decision to abandon the system.

3.1.3.8.4 Verify that the project team consistently applied accepted standards and criteria such as quality assurance, configuration management, and security in meeting its objectives.

3.1.3.8.5 Evaluate the RFP or similar solicitation documents for traceability of functions in the completed system to the requirements in the RFP.

3.1.3.8.6 Verify that the agency used "lessons learned" in the iterative process of developing the system.

3.1.3.9 Audit Products and Work Papers Developed in This Segment

3.1.3.9.1 Work papers summarizing the auditor's analysis of the reasonableness of management's decisions and the agency's documentation.

3.2 Custom Design, Development, and Deployment

The overall objective of this part is to describe the activities necessary to complete the design, development, and deployment of a customized system at one or more user sites with minimal disruption to routine (i.e., day-to-day operations). In general, key attributes that apply to most systems include:

- ease of use, including a short learning curve;
- security and confidentiality of sensitive data;
- availability;
- reliability (i.e., mean time to failure (MTTF));
- reasonable (i.e., short) for on-line systems;
- robustness (i.e., difficult to break);
- maintainability (i.e., flexibility of the design);
- survivability (i.e., resistance to external physical phenomena such as electrical surges, radiation); and
- cost-effectiveness.

This part can be applied to new system developments and modifications to existing systems. The custom approach has traditionally been used in the development of large complex systems. Typically, the custom approach used by federal agencies followed a method generally known as grand design. This is where an agency attempts to identify and define all of its functional, operational, and system requirements prior to system development. An example of this approach is DOD Mil-Std. 2167A; which is representative of the waterfall method and (2) Gane and Sarson's Structured Analysis and Design Technique.

The custom approach follows a clearly established process such as (1) defining user, business or mission requirements; (2) translating these requirements into functional and system specifications; (3) developing software to meet the functional and system specifications; (4) testing the software for adherence to functional and system requirements, including user acceptance; (5) deploying the system; and (6) operating and maintaining the system.

Users and agency management personnel should be closely involved with the designers and developers in this part. Users must approve the functional specifications that describe what the system will do from the user's viewpoint. They are also responsible for assisting designers and developers with defining the operational characteristics (i.e., batch, real-time, conversational, pseudo-real-time) and specifications for the system (i.e., security, data integrity, reliability). Designers use this information when considering alternative design approaches and managers use the information to update the project plan and revise estimates of project costs, benefits, schedule, and installation resources.

A key consideration in this part is the organizational barriers to the development and installation of the design once it is completed. As mentioned in the earlier phases, strategic

and tactical impediments caused by cultural or political factors need to be reevaluated with a view towards minimizing their negative effects.

There are three segments in the Custom Design, Development, and Deployment part:

- Needs Identification Segment: Identify and define, (1) the user, business or mission-related requirements; (2) the required automation capabilities; (3) the system features (i.e., architecture, data and information structure, flow and control); (4) the operational features (i.e., performance, security, and control features) that were developed in the concept and project initiation phase.

- System Design Segment: Based on the user needs identified in the previous segment, a team composed of both functional area specialists from the user community and system designers form the IRM community work cooperatively to develop the system design. This includes development of (1) the functional specifications for the system; (2) the characteristics of the operating environment; and (3) the technical design (i.e., system architecture, security provisions, reliability objectives).

- System Development and Deployment Segment: On the basis of an approved system design, a multi-disciplinary team of user representatives, designers, developers, and testers proceed with the development of the system using one or more conventional techniques (e.g., iterative or waterfall). This includes (1) detailed design and development at the subsystem, part, and unit levels; (2) development testing at all levels; (3) integration and operational testing; (4) independent validation and verification testing; and (5) user acceptance. Additionally, the team must plan and prepare for system deployment, including conversion and cutover, and initial operations (often referred to as initial operational capability--IOC). Deployment should proceed using a strategy and schedule that minimizes operational disruption in user sites.

Risk Management

Risk management plans should consider the risk factors identified in the earlier parts and proceed to refine those by further analyses. Additionally, a key consideration should be to determine whether the initial risk management plan is still applicable to this part.

Design and development of the system introduces additional vulnerabilities that may not have been previously considered. For example, the design might call for placing terminals in remote sites to increase the ease of data entry and access, but doing so may also increase the risk of unauthorized entry into the system. This risk should be addressed by placing controls over access to terminals and their usage. Each segment of this part may cause the overall risk management plan to be updated because each segment may introduce new potential risk

factors and vulnerabilities into the system. The risk management plan should help ensure that the necessary controls are established and enforced to mitigate against risks and threats.

Most risk management techniques are converted into detailed specifications during the design. For example, a selected risk control technique may be to have the system automatically select certain error-prone records for printout and manual review. A specification for this process may have been written previously, but would be incorporated into the overall design along with all other system specifications in this part.

Audit Staffing Considerations

The audit steps discussed in all segments of this part require, at a minimum, a general understanding of the agency's business and IRM concepts. Experience in systems analysis, design, and development would also be a valuable asset to the audit. GAO information systems analysts or ADP/telecommunications systems analysts knowledgeable in structured system analysis and design will be needed to evaluate the agency documents produced and the agency processes in this part.

The evaluator's knowledge base can be supplemented by intensive training in software engineering, structured systems analysis and design, and structured programming techniques. More basic supplemental training would include GAO or external courses in one or more of the following areas:

-- systems analysis,

-- introduction to information resources management,

-- systems development life-cycle management,

-- information systems security,

-- system maintenance, and

-- economic analysis.

Additional Considerations

If the agency has a quality assurance function (QA), it should obtain concurrence from QA on the project's technical and economic feasibility. It should also ensure that the approach used for developing the proposed system in this part is valid. The agency can also benefit from the use of an internal audit function for reviewing internal controls in this part.

Agency Profile

This part relies on the agency profile for information regarding the current IRM organization and standards, policies and procedures. Past reviews, audits, or studies may direct the audit team to deficiencies in the system development process. System profiles provide insight into the current IRM environment.

3.2.1 Needs Identification Segment

This is the first step in designing the proposed solution to satisfy the user's needs or the agency's mission. Using the documents developed in the concept and project initiation phase, the agency identifies specific user requirements and develops functional requirements (i.e., performance, business, security, and control features). The agency also reviews and updates the cost and schedule develops policies and procedures for transitioning to the proposed system and submits a proposal requesting management's approval to proceed.

3.2.1.1 Agency Objectives for This Segment

3.2.1.1.1 Identify, define, and document specific user requirements for performance, security, data and information management, and data integrity controls. Define deliverables, such as documents to be produced, communication networks, report formats, screen interfaces for operator and user purposes, and graphics.

3.2.1.1.2 If the agency does not have in-house expertise for developing the user requirements document, then the agency may contract with an external vendor to develop the requirements document, sometimes with the caveat that this contractor cannot bid to execute the project.

3.2.1.1.3 Develop and review policies and procedures that will support the transition to the new system.

3.2.1.1.4 Obtain management approval for the user requirements.

3.2.1.2 Relationship to Other Segments

This segment is initiated as a result of work in the Concept and Project Initiation phase for an existing system or a new project. The Needs Identification segment describes in greater detail the general nature of the business area and the problem to be solved or the enhancement that is needed. The information developed in this segment is the foundation for developing the functional and technical designs.

3.2.1.3 Agency Products and Documents Delivered During This Segment

3.2.1.3.1 High-level user requirements describing the general nature of the problem to be solved or the enhancement that is needed.

3.2.1.3.2 An overview of the current or proposed system, including a description of the architectural and operational features.

3.2.1.3.3 System functional requirements (i.e., translation of user requirements into specific system functions, such as screen displays, report formats, communication network requirements).

3.2.1.3.4 Project status reports.

3.2.1.3.5 Records of meetings between users, IRM, and management.

3.2.1.3.6 Project request document approving this segment.

3.2.1.3.7 A solicitation document if contractual support is required.

3.2.1.4 Management Responsibilities Discharged in This Segment

3.2.1.4.1 Authorize proceeding with this segment.

3.2.1.4.2 Provide resources (i.e., personnel, facilities, and funds) for this segment.

3.2.1.4.3 Develop a risk management plan, or if one already exists, update it using additional information collected in this segment.

3.2.1.4.4 Review and approve user requirements based on mission or programmatic necessity.

3.2.1.4.5 Ensure that IRM, contractors (if used), and user organizations work together to deliver user requirements and to allow users to verify and validate the user requirements.

3.2.1.4.6 In the event that contractual support is required, (1) develop a solicitation document (e.g., RFP) and (2) obtain a delegation of procurement authority (DPA) from GSA if required.

3.2.1.4.7 Ensure that the products generated in this segment, such as user requirements documentation, demonstrations, and proposals, are consistent with the agency's strategic and short-term objectives.

3.2.1.4.8 Ensure that support tools and the computing environment needed for developing user requirements and functional specifications are available.

3.2.1.4.9 Ensure that project milestones are being met or adjusted if necessary. Ensure that project costs are within the design-to-cost goals established. Ensure through peer review that products are accurate, complete, and represent high quality.

3.2.1.5 User Responsibilities Discharged in This Segment

3.2.1.5.1 Participate with the IRM group to develop and present the proposed functional and operational requirements to management for approval.

3.2.1.5.2 Specify performance, security, data integrity, and reliability control requirements.

3.2.1.5.3 Ensure that personnel with appropriate business and functional skills are available to execute this part.

3.2.1.5.4 Review and approve (i.e., verify and validate) the business area analysis for business systems or the required operational capability (ROC) for scientific and engineering systems.

3.2.1.6 IRM Responsibilities Discharged in This Segment

3.2.1.6.1 Participate, with the users, in the identification and definition of the user requirements and system functional specifications.

3.2.1.6.2 Develop, with user assistance, internal controls for security, data integrity, and system performance specifications.

3.2.1.6.3 Develop, with user assistance, the system characteristics and features.

3.2.1.6.4 Identify and develop, with user participation, the database requirements.

3.2.1.6.5 Identify and develop, with user participation, any networking and telecommunication requirements.

3.2.1.6.6 Establish, with user participation, procedures for manual and automated processes (e.g. on-line versus batch processing).

3.2.1.6.7 Prepare and present progress and status reports to management.

3.2.1.6.8 Develop a solicitation document (e.g., RFP) for contractual support if necessary. Formally coordinate with the users. Forward the solicitation document to management for approval.

3.2.1.7 Audit Objectives During This Segment

3.2.1.7.1 Verify that the user and functional requirements have been adequately defined and validated.

3.2.1.7.2 Determine whether the agency has established a development team involving users and IRM staff with the appropriate skills.

3.2.1.7.3 Determine whether the agency has allocated the appropriate resources (i.e., funding and automation) for this project.

3.2.1.7.4 Determine that the agency has thoroughly identified, defined, and documented its requirements.

3.2.1.8 Audit Tasks for This Segment

3.2.1.8.1 Determine that the user's functional and operational requirements were appropriately derived using conventional techniques such as business area analysis.

3.2.1.8.2 Assess whether the user requirements document is unambiguous, complete, verifiable, consistent, modifiable, and traceable (ANSI/IEEE Standard 830-1984). Definitions for these terms are given below:

a. Unambiguous: The requirements specification or business area analysis document is unambiguous, if and only if, every requirement stated in it has only one interpretation. As a minimum, this requires that each characteristic of the final product be described using a single term. In cases where a term used in a particular context may have multiple meanings, the term must be included in a glossary where its meaning is made more specific.

b. Complete: A requirements specification or business area analysis document is complete if it has the following qualities:

   -- inclusion of all significant requirements, whether in relation to business area processes affected and to be changed, user functions, performance, architectural and organizational constraints, and interfaces with other systems;

   -- definition of realizable (legitimate) classes of input information and valid responses including exceptions;

   -- full labeling and referencing of all figures, tables, and diagrams in the document and definition of all terms and units of measure; and

   -- should not use "to be determined" (TBD) phrases except in cases where accompanying explanations are attached (e.g., "to be determined in the next version of this document").

c. Verifiable: A requirement or business area analysis is verifiable if, and only if, every requirement stated in these documents has a finite cost-effective process with which a person or machine can check that the document meets the requirement.

d. Consistent: A document is consistent if and only if no set of individual requirements described in it conflict with any other set of requirements.

e. Modifiable: A requirements or specification document is modifiable if and only if its structure and style is such that any necessary changes to it can be made easily, completely, and consistently. Modifiable generally refers to a document that:

   -- has a coherent and easy-to-use organization, with a table of contents, an index, and explicit cross-referencing to other relevant documents; and

   -- is not redundant; that is, the same requirement should not appear in more than one place in the user requirements specification.

f. Traceable: A requirements specification is traceable if, and only if, each requirement can be referenced in relevant precursor documents and in documents that are created after the one whose traceability is in question (that is "backward traceability" and "forward traceability").

3.2.1.8.3 If the agency has established the use of software development tools, obtain the agency's guidelines for using such tools and determine whether both guidelines and these tools were used for developing the user requirements.

3.2.1.8.4 Identify the unique features that contribute to high risk of failure in identifying user requirements and assess whether agency management has taken steps to address these in the risk management plan. If not, then this is a finding.

3.2.1.8.5 Evaluate sensitivity analyses for approximate costs and schedules.

3.2.1.8.6 Verify that management consistently applied the agency's internal controls, generally accepted standards, and criteria in meeting the objectives of this segment.

3.2.1.8.7 Independently analyze cost and schedule reports using cost estimation tools such as COCOMO or SLIM to verify that the reported costs and schedules are similar to those derived using these tools.

3.2.1.8.8 Determine whether appropriate staff, skills, and computing resources were available to the project team.

3.2.1.8.9 Verify that the entity obtained management approval before proceeding to the next segment.

3.2.1.8.10 Evaluate solicitation documents for anomalies, inconsistencies, and reasonableness. (See GAO/IMTEC 8.1.6.)

3.2.1.9 Audit Products and Work Papers Developed in This Segment

Work papers summarizing the evaluation team's analysis of:

3.2.1.9.1 the user's derivation of the functional and operational requirements;

3.2.1.9.2 the consistency and traceability of the user requirements and system functions;

3.2.1.9.3 agency-developed sensitivity analyses (i.e., relaxing several assumptions or constraints that influenced the requirements determination) of the user requirements, if performed.

3.2.1.9.4 the agency's risk management plan for mitigating project risks; and

3.2.1.9.5 the reasonability of the agency's staffing considerations.

BLANK PAGE

3.2.2 System Design Segment

This segment outlines the expectations, duties, and responsibilities for the agency and outlines duties and responsibilities of the audit function. The system design document (1) defines the system functions; (2) communicates this information using either business (i.e., insurance, banking, payroll) or mission area (i.e., command and control, intelligence, electronic warfare, space) terminology; and (3) defines the technical attributes of the system including the system architecture, logical and physical database structure, telecommunications network topology, and application software structure.

3.2.2.1 Agency Objectives for This Segment

3.2.2.1.1 Define all of the inputs and outputs to the system.

3.2.2.1.2 Define processing functions that will manipulate the data.

3.2.2.1.3 Develop the system design specification.

3.2.2.1.4 If appropriate, develop a solicitation document to acquire contractual support. Obtain management approval of the solicitation document.

3.2.2.1.5 Management and users sign off on the system design specification.

3.2.2.1.6 Define the overall system architecture.

3.2.2.1.7 Define constraints that could affect the selection of technical architectures.

3.2.2.1.8 Document the type and extent of training needed to control and support the proposed technical environment.

3.2.2.1.9 Convert functional specifications into application program specifications.

3.2.2.1.10 Analyze the feasibility of the system design (i.e., functional and technical) relative to the overall functional and operational requirements.

3.2.2.1.11 Identify the human interfaces to the system and the procedures required to support these interfaces.

3.2.2.1.12 Estimate project team and user training necessary to complete the design, development, installation, and operation of system.

3.2.2.2 Relationship to Other Segments

3.2.2.2.1 The system design specifications created in this segment should be consistent with and build upon the user requirements developed in the previous segment. The iterative part can be used to provide feedback to the previous segment as well as expedite the development of a working prototype in the next segment.

3.2.2.2.2 Overall system design (i.e., functional and technical) is the point at which enough information is known with regard to the specific attributes of the system that the rough cost and schedule estimates previously derived can be substantially refined. For many agencies, several technical architecture decisions may have already been defined in the planning phase or by the existence of a preexisting base of applications that do not need significant change to be adapted to the new system environment.

3.2.2.3 Agency Products and Documents Delivered During This Segment

3.2.2.3.1 System design specifications.

3.2.2.3.2 Project status reports.

3.2.2.3.3 Minutes of meetings held by all players involved with the system design.

3.2.2.3.4 Relevant project approval documents.

3.2.2.3.5 A solicitation document for contractual support, if required.

3.2.2.3.6 Technical architecture, including a definition of (1) how each user function will be achieved; (2) where the functions will be processed; (3) how the data will be communicated; (4) the interfaces to other application systems; (5) the generalized screen designs; (6) the hardware platform(s) required to support the functional and operational requirements; and (7) the required support software (i.e., task handler, screen handler, diagnostic aids).

3.2.2.3.7 Telecommunications network topology including local area networks, metropolitan area networks, and wide area networks.

3.2.2.3.8 Logical and physical database design specifications.

3.2.2.3.9 Software development strategy based on an approved system design.

3.2.2.3.10 Performance expectations (i.e., from a functional and operational service-level perspective, or from an end item (i.e., tank, missile, aircraft) performance level perspective) for the recommended design and other alternative designs considered by technical design team.

3.2.2.4 Management Responsibilities Discharged in This Segment

3.2.2.4.1 Approve a particular strategy for system development and installation. Approaches to be reconsidered are the iterative development and installation method and the packaged system (i.e., commercial off-the-shelf program products) method.

3.2.2.4.2 Ensure use of agency accepted policies, methods, standards, and tools for the development of user design specification.

3.2.2.4.3 Provide the resources and skill levels needed to develop the system design.

3.2.2.4.4 Review and approve the overall system design, taking into account risks and affordability.

3.2.2.4.5 Monitor progress of the project.

3.2.2.4.6 Review and approve proposed service levels required by user.

3.2.2.4.7 Review and approve the approach for security, data integrity, and application controls.

3.2.2.5 User Responsibilities Discharged in This Segment

3.2.2.5.1 Work with IRM to further clarify (1) the definitions and logical representations of the inputs and outputs; (2) the database schema and sub-schema; (3) the information required for management reports, production operations, etc.; and (4) other system capabilities to satisfy business needs.

3.2.2.5.2 Review and concur with the system design specifications.

3.2.2.5.3 Define required system performance and service levels.

3.2.2.5.4 Define security, data integrity, and audit trail control requirements.

3.2.2.5.5 Assist IRM in evaluating technical architecture options and tradeoffs.

3.2.2.5.6 Assist IRM in defining all interfaces (i.e., human and another AIS) to the system.

3.2.2.6 IRM Responsibilities Discharged in This Segment

3.2.2.6.1 Work with users to refine specifications for security, data management, system performance, and system reliability.

3.2.2.6.2 Perform, with user assistance, "event analysis" studies to detect missing user functions.

3.2.2.6.3 Refine, with user participation, user processing needs.

3.2.2.6.4 If contractual support is required, work with the users to develop the solicitation document and obtain management approval.

3.2.2.6.5 Prepare and present progress reports to management.

3.2.2.6.6 Ensure the integrity of the system design specifications through peer reviews.

3.2.2.6.7 If software development tools and standard methodologies are in place, follow agency guidelines and accepted practices for using such tools to develop the system design.

3.2.2.6.8 If quality assurance or internal auditor functions are in place, then obtain concurrence from QA and internal auditor on the consistency and completeness of the transition from the user functional and operational requirements to the system design specification (i.e., requirements traceability).

3.2.2.6.9 Prepare the technical architecture specification.

3.2.2.6.10 Determine the telecommunications network topology and design the network.

3.2.2.6.11 Design the logical and physical database structures.

3.2.2.6.12 Design the application programs including modules, subroutines, and functions.

3.2.2.6.13 Update the risk analysis taking into account the attributes of the overall system design.

3.2.2.6.14 Develop preliminary test plans based on system design specifications and functional and operational requirements.

3.2.2.7 Audit Objectives During This Segment

3.2.2.7.1 Determine whether the agency performed and documented the work necessary to meet the objectives of this segment.

3.2.2.7.2 Determine whether the system design specification meets the functional and operational requirements for the system.

3.2.2.7.3 Evaluate the risk management plan and any supporting risk analyses that cover particular attributes of the system design specification.

3.2.2.7.4 Determine whether the proposed technical architecture is consistent with the agency's new concept of operations.

3.2.2.7.5 Verify that adequate consideration was given to continuity of operations (i.e., disaster recovery and routine outages) for key user processes.

3.2.2.8 Audit Tasks for This Segment

3.2.2.8.1 Draw a sample from the overall system specifications and trace them back to supporting functional and operational requirements. As a short cut, agency management can be asked for such a document from their quality assurance or oversight group.

3.2.2.8.2 Verify that the risk management plan has been updated per the refinements identified in the system design specification.

3.2.2.8.3 Verify that the agency has evaluated the impact of the system design specifications on the estimated cost and schedule for the program or project.

3.2.2.8.4 Verify agency compliance with applicable policies, procedures, and standards.

3.2.2.8.5 If appropriate, evaluate the quality of the solicitation document.

3.2.2.8.6 Determine whether the technical architecture is consistent with the agency's new concept of operations.

3.2.2.8.7 Assess the agency's system design for ambiguities, completeness, consistency, maintainability, robustness, traceability, and usability.

3.2.2.8.8 Verify that adequate consideration was given to continuity of operations (i.e., disaster recovery and routine outages) for key user processes.

3.2.2.9 Audit Products and Work Papers Developed in This Segment

Work papers summarizing the evaluation team's analysis of:

3.2.2.9.1 documents describing the agency's design methodology, techniques, and tools used;

3.2.2.9.2 the traceability of functional and operational requirements to the system specification;

3.2.2.9.3 a sample of the system design specifications for technical integrity;

3.2.2.9.4 the technical architecture and alternatives;

3.2.2.9.5 the revised economic analysis and schedule estimates;

3.2.2.9.6 the risk management plan and any supporting risk analyses.

3.2.3 System Development and Deployment Segment

This segment defines system development (i.e., software development, integration, test and evaluation) and deployment (i.e., initial operational capability and full deployment) activities to be taken by the agency and outlines duties and responsibilities of the audit function.

3.2.3.1 Agency Objectives for This Segment

3.2.3.1.1 Translate the system design specifications into computer software (i.e., application programs which are often referred to as code, and/or databases which consist of data elements, records, and files) using a standard software engineering environment.

3.2.3.1.2 Establish and implement a software quality assurance function.

3.2.3.1.3 Develop and implement unit, integration, and system test plans.

3.2.3.1.4 Ensure that an independent verification and validation of the system is conducted.

3.2.3.1.5 Ensure that user acceptance tests are conducted.

3.2.3.1.6 Place approved products (i.e., design specifications, application programs, documentation) under configuration control.

3.2.3.1.7 Ensure that the system is still affordable and cost effective.

3.2.3.1.8 Develop and implement a transition strategy that covers elements such as conversion preparation; conversion and cutover; documentation (i.e., maintenance manuals, user manuals, operations manuals) preparation; and fallback procedures.

3.2.3.1.9 Develop and implement installation plans for IOC and full scale deployment.

3.2.3.1.10 Determine if contractual support is required. If so, develop and obtain management approval for a solicitation document (i.e., RFP and IFB).

3.2.3.1.11 Develop and implement acquisition plans for the procurement of required computer equipment, telecommunications equipment, and commercial software products which are often referred to as commercial off-the-shelf (COTS) products.

3.2.3.2 Relationship to Other Segments

3.2.3.2.1 The application system created in this segment and its supporting computer equipment, telecommunications equipment, and commercial software should be consistent with the system specifications developed in the previous segment. Techniques from the iterative part can be used to provide feedback to the previous segment as well as expedite the development of a working prototype.

3.2.3.2.2 Installation planning, initial operating capability, and full-scale deployment must be consistent with the new concept of operations. Suitability of the system for operations depends on many factors including: ease of use, reliability, and security.

3.2.3.3 Agency Products and Documents Delivered During This Segment

3.2.3.3.1 Organization charts showing federal agency, program office, and supporting contractors.

3.2.3.3.2 Policies, procedures, and standards applicable to the project.

3.2.3.3.3 Completed work plan (i.e., work breakdown structure) with human resources, scheduling, and funding for each step.

3.2.3.3.4 Programming specifications including:

a. data-flow diagrams, state transition diagrams, and computer program logic diagrams;

b. cross-references to database data structures (information elements/items in database) and logical and physical file structure descriptions; and

c. input/output and screen formats.

3.2.3.3.5 A program development and test library.

3.2.3.3.6 A test analysis report that validates and verifies the quality of the application software. The software should be of production quality and suitable for operations in a user facility. Note: An exception to this item is when a user site agrees to take on the risk of participating in product improvement as an "alpha" or "beta" test site.

3.2.3.3.7 A library of production quality application software that has been placed under configuration control.

3.2.3.3.8 System support documentation including maintenance manuals, user manuals, operations manuals, technical reference manuals.

3.2.3.3.9 Training schedule and course materials for management, users, and IRM personnel. Course materials can include software tutorials and self-paced training material.

3.2.3.3.10 A transition plan including conversion from the legacy environment to the replacement system.

3.2.3.3.11 Telecommunications network management plan, if applicable.

3.2.3.3.12 A deployment plan including site surveys, site preparation, installation schedule, user acceptance.

3.2.3.3.13 Installed computer and telecommunications equipment (i.e., mainframes, servers, micros, concentrators, front-end processors, switches, printers), and a software engineering environment (i.e., operating systems, assemblers, loaders, simulators, emulators, compilers, interpreters, database management systems).

3.2.3.3.14 Continuity of operations plan (i.e., disaster recovery and routine operational outages) and procedures.

3.2.3.3.15 Performance measures that link to the users' operations.

3.2.3.4 Management Responsibilities Discharged in This Segment

3.2.3.4.1 Review and approve the development approach to be used during this segment.

3.2.3.4.2 If a contractor has been selected to design and develop the system, ensure that a team has been organized to review and monitor critical aspects of the development activity (i.e., computer program specifications, unit test results, integration test results).

3.2.3.4.3 Conduct progress reviews for adherence to the cost and schedule expectations and approve any adjustments that may be required.

3.2.3.4.4 Establish performance measures (e.g., robustness index, responsiveness, and inherent security of the developed code) that are oriented towards product quality and monitor progress against these objectives.

3.2.3.4.5 Review and approve requests for changes to system requirements.

3.2.3.4.6 Ensure that quality assurance and appropriate standards for structured programming techniques, coding, communication interfaces, walkthroughs, reviews, and databases have been implemented.

3.2.3.4.7 Review and approve the system test and conversion plans.

3.2.3.4.8 Ensure that formal verification and validation of the developed system occurs.

3.2.3.4.9 Review and approve formal releases of the system.

3.2.3.4.10 Ensure that the appropriate software engineering environment is in place for use by the project team.

3.2.3.4.11 For projects using the incremental development technique, review and approve the release of each operational increment. This includes the release to alpha and beta sites also.

3.2.3.4.12 Review and approve the transition plan including procedures for site surveys, conversion preparation, and contingencies.

3.2.3.4.13 Agreement that acceptance test results meet management's criteria.

3.2.3.4.14 Conduct formal milestone reviews (i.e., critical design review, functional configuration audit, formal qualification review) to ensure adherence to structured system design and development techniques.

3.2.3.4.15 Review and approve the training plan.

3.2.3.5 User Responsibilities Discharged in This Segment

3.2.3.5.1 Communicate with management and IRM organizations to determine the status of the project. If problems cause delays, users should be aware of the reasons for such delays and assist whenever possible to resolve issues that cause delays.

3.2.3.5.2 Participate in verification and validation of system functions.

3.2.3.5.3 Provide staff to project team to ensure user participation during implementation and installation.

3.2.3.5.4 Jointly, with the IRM staff, develop system support products (e.g., user manuals, user aids, on-line help procedures) a training plan, and course materials for potential users.

3.2.3.5.5 Define system test conditions (i.e., functional and operational performance expectations) and necessary test data. Ensure that test conditions are representative of the extended environment.

3.2.3.5.6 Assist the IRM staff in the verification of system test results.

3.2.3.5.7 Assist the IRM staff in the development of the overall transition strategy and plan including legacy database cleanup, conversion procedures, and site preparation.

3.2.3.5.8 Assist the IRM staff in the review and control of system change requests. Recommend a prioritization strategy to management for approval and enforcement.

3.2.3.5.9 Participate with IRM staff in acceptance testing of any computer or telecommunications equipment that will be installed in user areas.

3.2.3.5.10 Assist the IRM staff in collecting information on system costs incurred and benefits realized.

3.2.3.6 IRM Responsibilities Discharged in This Segment

3.2.3.6.1 If contractual support is required, work with the users to develop the solicitation document and obtain management approval.

3.2.3.6.2 Develop the detailed design specifications including computer program specifications, interface specifications, and communication software specifications.

3.2.3.6.3 Develop the applications software (i.e., code, unit test, unit and subsystem level integration).

3.2.3.6.4 Test the program modules individually and in an integrated mode, resolving as many computer program logic, data definition and representation, and computer program interface problems as possible.

3.2.3.6.5 Develop the test and conversion plans and test-beds.

3.2.3.6.6 Install system software and hardware as necessary.

3.2.3.6.7 Document all changes to the detailed design specifications, code, and procedures that may have been required during the testing of program modules.

3.2.3.6.8 Assist management with overall quality assurance by using techniques such as peer reviews of computer program specifications, structured walkthroughs of code.

3.2.3.6.9 Inform management of potential software development and test problems that may adversely affect the estimated costs or schedule.

3.2.3.6.10 Take advantage of any hardware reutilization or software reuse opportunities that are feasible.

3.2.3.6.11 Ensure that the development team has the complement of skills (i.e., functional, operational, and technical) to accomplish the system design objectives.

3.2.3.6.12 Develop a deployment plan including (1) logistics, (2) training, and (3) procedures (i.e., operations, users, and user support).

3.2.3.6.13 Conduct system integration tests in an environment that simulates user site characteristics to the extent feasible.

3.2.3.6.14 Jointly with users, conduct a full system test, including stress testing in an actual user environment, if feasible. Note: Sometimes alpha sites are established to test a particular concept of operations, particularly if the iterative technique is used. Similarly, beta sites may be established to test for system stability under a wide variety of circumstances (e.g., differences in environmental conditions, variations in type and volume of activity, and variations in standards of practice). Particular attention should be placed on issues such as system reliability and responsiveness, data integrity and security, and ease of use.

3.2.3.6.15 Jointly with users, develop the system validation and verification plans and procedures.

3.2.3.6.16 With management approval, ensure that an independent team conducts the validation and verification tests.

3.2.3.6.17 Ensure that exception reports for functions or features that do not operate as expected are documented and reported to management for approval of suggested corrective actions prior to full conversion from the legacy environment to the new environment.

3.2.3.6.18 Ensure that the end products of system development (i.e., detailed design specifications, application programs, system documentation) are placed under configuration control.

3.2.3.6.19 Jointly with users, update the economic analysis for the system including a revised forecast of the life-cycle costs. Any benefits (tangible and intangible) should be documented at this time.

3.2.3.6.20 Obtain management approval for the resources required to perform the conversion and cutover to the new system. Also obtain management approval for the funding and human resources required for continued system operations and maintenance in the upcoming budget year and beyond.

3.2.3.6.21 Document the test results for all critical operational initiatives that serve as prerequisites to full-scale deployment and obtain management approval for the resolution of outstanding issues.

3.2.3.6.22 Define the resources that will be required for operations and maintenance of the system.

3.2.3.7 Audit Objectives During This Segment

3.2.3.7.1 Determine whether the agency designed, developed, tested, and deployed the automated system required by the user organization in accordance with (1) applicable federal laws, regulations, and standards; (2) agency policies, procedures, and standards; and (3) conventional management and technical practices.

3.2.3.8 Audit Tasks for This Segment

3.2.3.8.1 Obtain updated organizational charts.

3.2.3.8.2 Determine whether relevant program and project management plans have been updated. These plans should include updated cost estimates, schedules, and tasks.

3.2.3.8.3 Verify that the agency complied with the relevant federal laws, regulations, and standards as well as agency specific policies, procedures, and standards.

3.2.3.8.4 If appropriate, evaluate the quality of the solicitation document.

3.2.3.8.5 Verify that program and project risks were reduced through the use of conventional system development tools (i.e., computer aided design (CAD), computer aided software engineering (CASE), and fourth generation languages) and techniques (i.e., peer reviews, structured walkthroughs, formal inspection).

3.2.3.8.6 Obtain the overall system design document, and the detailed system, subsystem, module, computer program, or database specifications, if required.

3.2.3.8.7 Evaluate the agency process for the acquisition of COTS products (i.e., computer equipment, communications equipment, and software). Verify that the products acquired are supported by the system architecture, design, and operating characteristics. Also verify that system integration issues associated with COTS products have been resolved.

3.2.3.8.8 Evaluate the impact (i.e., technically, operationally, and financially) of agency modifications to COTS products. Verify that the modifications were clearly documented and communicated to management.

3.2.3.8.9 Evaluate the agency's software engineering processes for critical attributes (i.e., key process areas) such as software configuration management, software subcontract management, and software quality assurance. Note: Consult with the chief scientist for assistance from a software capability evaluation (SCE) team.

3.2.3.8.10 Verify that testing was done in accordance with the test plan approved by agency management.

3.2.3.8.11 Verify the existence and evaluate the adequacy of the various planning documents (i.e., transition plan, training plan, deployment plan) produced during development and deployment.

3.2.3.8.12 Verify that the agency's derivation of the estimated costs and schedule is reasonable (i.e., supportable through the use of tools, deductive logic, conventional industrial cost estimating techniques).

3.2.3.8.13 Verify that the detailed design contains no anomalies or inconsistencies relative to the technical and functional specifications developed during the Design segment.

3.2.3.8.14 Verify that plans for testing and conversion were developed during this segment. Evaluate these plans for accuracy, completeness, and realism.

3.2.3.8.15 Verify the results of the various levels of testing (i.e., unit, integration, or system) for consistency with performance requirements defined during the System Design segment. This would include concerns such as (1) system response time; (2) peak workload (i.e., stress) processing; and (3) operational performance sensitivity to the choice of language or database characteristics.

3.2.3.8.16 Obtain a copy of various test analysis reports, if available.

3.2.3.8.17 Verify that a thorough and complete verification and validation of the system developed in this segment was done by the agency.

3.2.3.8.18 Evaluate the operational readiness of (1) the system; (2) the user environment to receive the system; and (3) the operational and maintenance support environment for the system. Operational readiness issues include (1) the resolution of all critical and most high-priority system problem reports; (2) the completion of initial training for the first group of users to receive the system; and (3) the establishment of a rigorous hardware and software configuration control process for sustainability (i.e., overall system maintenance and support).

3.2.3.8.19 Evaluate the effectiveness of the agency's conversion from the legacy environment to the new system. Check for (1) the accuracy and completeness of the data conversion; (2) revisions and replacements of old procedures; and (3) training and indoctrination processes for users of the new system.

3.2.3.8.20 Evaluate the reasonableness of contingency plans.

3.2.3.8.21 Evaluate the impact of managerial decisions throughout the development and deployment of the system. Also focus on the continued affordability of the system.

3.2.3.8.22 Evaluate the existence and determine the adequacy of operationally oriented performance measures for the programmatic area(s) affected. In lieu of performance measures, agencies may periodically perform benefit realization studies, program evaluations, in-process reviews, etc.

3.2.3.9 Audit Products and Work Papers Developed in This Segment

Work papers summarizing the evaluation team's analysis of:

3.2.3.9.1 the program or project management plans;

3.2.3.9.2 the revised economic analysis and schedule estimates;

3.2.3.9.3 the risk management plan and any supporting risk analyses;

3.2.3.9.4 agency system design and development specification documents;

3.2.3.9.5 the adequacy of the software development, quality assurance, configuration management, and independent verification and validation plans;

3.2.3.9.6 agency test plans and test analysis reports;

3.2.3.9.7 agency system transition and cutover plans;

3.2.3.9.8 agency deployment plans and actions; and

3.2.3.9.9 the adequacy of management actions.

Contents of the Operations and Maintenance Phase

4.0 The System Operations and Maintenance Phase

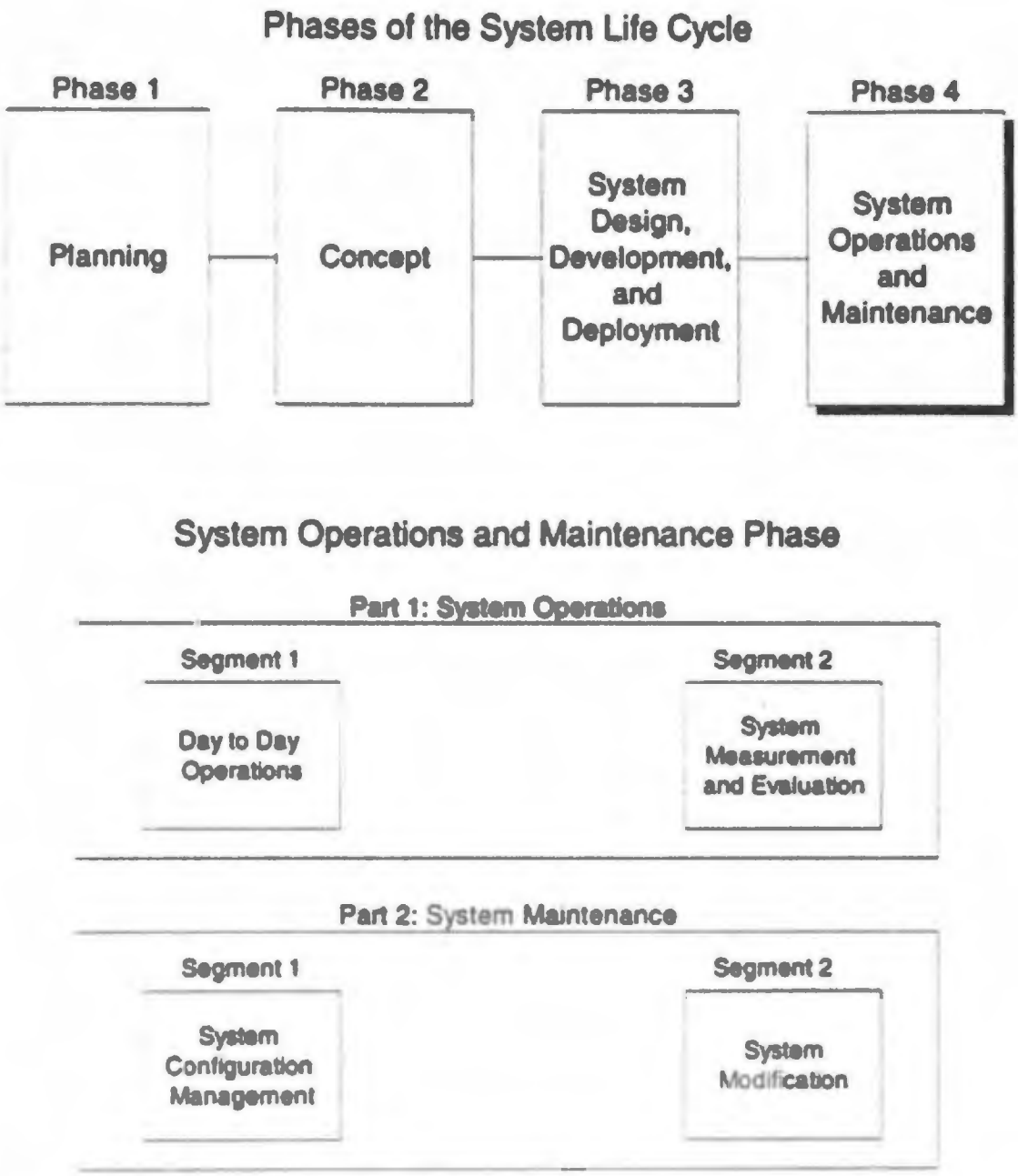

Figure 6. The System Operations and Maintenance Phase

The system operations and maintenance phase begins after deployment and system activation at each site. Management responsibility is transferred from the project manager to the operations manager and ends when the system is replaced by a new system or is terminated. Key activities during this phase include:

-- operation and maintenance of the computer and telecommunications equipment;

-- maintenance of system and support software;

-- maintenance and modification of application software;

-- configuration management of the software and hardware;

-- evaluation of the system's effectiveness and benefits;

-- sustaining system stability and effectiveness through post-deployment modernization activities; and

-- replacement of the system when the existing system has reached the end of its useful life (i.e., return to the planning phase).

This phase is presented in two parts (1) system operations and (2) system maintenance. System operations is concerned with day-to-day operations and system performance and measurement. From a hardware perspective, system operations also covers preventive maintenance. System maintenance covers remedial (i.e., corrective) maintenance, adaptive maintenance, and perfective maintenance. These four maintenance activities are defined in the following manner:

-- Corrective Maintenance - this activity occurs because it is unreasonable to expect that software testing will uncover all latent errors in a large software system. The corrective maintenance process includes the diagnosis and correction of these errors.

-- Adaptive Maintenance - this activity, which modifies the software to properly interface with a changing hardware, operating system, and peripheral equipment, environment is not only commonplace but also necessary.

-- Perfective Maintenance - this activity accounts for the majority of all the efforts expended on software maintenance. As the software is used, requests for new capabilities, modifications to existing functions, and general enhancements are received from users. To satisfy these requests, the perfective maintenance activity is performed.

-- Preventive Maintenance - this activity occurs when changes to the software are needed to improve maintainability, reliability, or to provide a better basis for future enhancements.

These activities are covered within the context of system configuration management and system modification. Emphasis is placed on the operation, maintenance, and modification of software.

BLANK PAGE

4.1 System Operations

System operations is where the appropriate organizational units of an agency take ownership and responsibility for operating the new system. It is concerned with ensuring effective, efficient, and economical day-to-day operations and continuity of operations including disaster recovery and an effective problem-management process. System operations must be performed in a controlled environment in accordance with the agency's policies, standards, and procedures, as well as conform to operating plans, budgets, and legal and regulatory requirements.

This part contains the following two segments:

- day-to-day operations segment: Perform the tasks and processes necessary to operate the system on a daily basis to fulfill agency mission and program objectives. This includes continuity of operations and problem management.

- system measurement and evaluation segment: Measure and evaluate the system's performance in terms of its compliance with policies, procedures, standards, and other operational criteria that govern its responsiveness to programmatic goals and objectives.

For each of these segments, the agency must manage the following functions, activities, and system components:

- input and output control
- production scheduling and operation
- system performance management
- system availability and reliability
- systems software
- configuration management
- telecommunications
- end-user computing
- security
- storage media management
- training

Risk Management

The agency should establish policies, procedures, and standards for identifying vulnerabilities and potential threats to the system and assessing risk. It should ensure that the necessary controls and protective measures are implemented to reduce risk to acceptable levels. The

agency should also ensure that these policies, procedures, and standards are properly documented, clearly communicated, and well understood.

Performing a risk assessment in the operational environment addresses the following vulnerabilities:

-- lack of adequately trained personnel;

-- unrealistic operating schedules and budgets;

-- ineffective fallback procedures for operational disruptions that are not caused by major disasters;

-- ineffective physical, administrative, or technical access controls to the system;

-- ineffective management of a multi-vendor environment;

-- system performance shortfalls such as (1) excessive downtime, (2) slow response time, and (3) long system restoration periods.

Agency Profile

This part relies on the agency profile for information regarding the current IRM organization and standards, policies and procedures. Past reviews, audits or studies may direct the audit team to deficiencies related to system operations. System profiles provide insight into the current IRM environment.

4.1.1 Day-to-Day Operations Segment

The information resources and processes associated with day-to-day operations are driven by the operating plan. Information resources include computer and telecommunications hardware and software; information products and services; personnel; and facilities (i.e., data center, network control center, operations support center). Processes include workload management, media management, and user support.

To be effective, a system should operate as intended and provide users with the information and services they need to fulfill program objectives and agency missions and goals. System services and information should meet the users' needs for timeliness, accuracy, completeness, reliability, security, and survivability. Systems should conserve resources (i.e., disk consumption, communications capacity, human interfaces) to the extent practical and attempt to optimize the consumption of such resources.

Information systems security and the presence of internal controls are essential to protect the integrity, confidentiality, and availability of information, data, and other systems resources during day-to-day operations. Weak or ineffective implementation of contingency plans, security procedures, and internal controls exposes the system to risks of unauthorized access, accidental loss, fraud, waste, abuse, and mismanagement.

4.1.1.1 Agency Objectives for This Segment

4.1.1.1.1 Ensure that operating plans are being implemented effectively and that budgets realistically allow for day-to-day operations, including continuity of operations.

4.1.1.1.2 Ensure that policies and procedures for input and output are being implemented.

4.1.1.1.3 Manage facility operations in centralized or distributed processing centers, including management of data centers, network control centers, and customer support centers.

4.1.1.1.4 Coordinate with maintenance staff to update or replace system resource components (i.e., computer equipment, system software, communications equipment) when required.

4.1.1.1.5 Operate and manage telecommunications resources.

4.1.1.1.6 Provide support (i.e., help desk, diagnostic assistance, general indoctrination) to end users in an appropriately controlled environment.

4.1.1.1.7 Manage and implement security policies and procedures.

4.1.1.1.8 Provide sufficient training for operations personnel.

4.1.1.2 Relationship to Other Segments

In this segment, the agency manages the system and other information resources according to an approved set of operating plans, policies, procedures, and standards. In the following segments, the agency measures system performance and evaluates overall operational efficiency and effectiveness.

4.1.1.3 Agency Products and Documents Delivered During This Segment

4.1.1.3.1 Updated and current operations and procedures manuals.

4.1.1.3.2 Periodic risk analyses.

4.1.1.3.3 Periodic budget, cost-benefit, and operational performance analyses.

4.1.1.3.4 Periodic performance indicators and trends.

4.1.1.4 Management Responsibilities Discharged in This Segment

4.1.1.4.1 Ensure that sufficient resources are available to operate the system.

4.1.1.4.2 Manage the resources committed to or used in operating the system, e.g., dollars, personnel, and contractual support and obligations.

4.1.1.4.3 Ensure that an effective security awareness program is operational and that agency personnel are properly trained in matters relating to security.

4.1.1.4.4 Ensure that internal controls are established and followed.

4.1.1.4.5 Manage exceptions to standard operating procedures and the use of standard products.

4.1.1.4.6 Ensure that the IRM unit is satisfying user needs.

4.1.1.4.7 Ensure that end-user applications conform to plans, budgets, internal controls, policies, standards, and procedures.

4.1.1.4.8 Review and approve updates to operating plans, budgets, policies, standards, and procedures.

4.1.1.4.9 Ensure that agency personnel are properly trained to operate the system effectively, efficiently, and economically.

4.1.1.4.10 Ensure that IRM and users agree to changes in technology and that such changes are introduced in a controlled manner.

4.1.1.5 **User Responsibilities Discharged in This Segment**

4.1.1.5.1 Ensure that user clearly understand their missions as currently assigned by law, regulation, or agency management and establish operating plans and procedures for implementing their missions.

4.1.1.5.2 Establish work performance agreements with IRM.

4.1.1.5.3 Utilize resources (hardware, software, data, and personnel) in an effective, economical, and efficient manner to meet missions and objectives.

4.1.1.5.4 Maintain and manage information that supports the agency's mission, program objectives, and policies.

4.1.1.5.5 Work with IRM to ensure that information and system services are complete, accurate, reliable, secure, and timely.

4.1.1.5.6 Submit input data in accordance with published schedules and established operating procedures.

4.1.1.5.7 Verify the results of processing.

4.1.1.5.8 Grant access to programs and data on a need-to-use basis and report access violations to the security administrator.

4.1.1.6 **IRM Responsibilities Discharged in This Segment**

4.1.1.6.1 Operate and control systems resources in an effective, economical, and efficient manner.

4.1.1.6.2 Schedule and monitor input/output tasks and other automated information system support activities, such as the scheduling of job streams, as appropriate.

4.1.1.6.3 Provide users with necessary information products and services to meet missions and objectives.

4.1.1.6.4 Identify and resolve environmental problems (e.g., humidity, air conditioning, power) that affect operations and communicate these to management.

4.1.1.6.5 Control the media library and the movement and usage of storage media.

4.1.1.6.6 Ensure system availability, reliability, responsiveness, etc. Also, take the necessary actions to ensure continuity of operations.

4.1.1.6.7 Identify alternative and new technologies that can be applied to improve operational effectiveness and assist management in its selection.

4.1.1.7 Audit Objectives During This Segment

4.1.1.7.1 Determine whether system operations are (1) supporting the user's role in carrying out agency mission and program objectives and (2) providing users with complete, accurate, timely, reliable, and usable information and data.

4.1.1.7.2 Determine how well the agency is managing operating costs, and whether it is effectively, efficiently, and economically controlling any contractual arrangements and the use of information resources.

4.1.1.7.3 Verify that an appropriate control environment is in place to ensure that information resources are adequately safeguarded against accidental loss, theft, unauthorized access, fraud, waste, and abuse.

4.1.1.8 Audit Tasks for This Segment

4.1.1.8.1 Review the agency and system profiles and update them if necessary. Verify that the computer equipment, system software, communication equipment, communications software, production job streams, cataloged applications, hardware configuration, network topology, and overall system architecture are documented and understood by the evaluation team.

4.1.1.8.2 Identify the internal and external information flows, services, and products that are critical to the success of the federal program or activity under study and assess whether the system effectively supports these flows, services and products. Ask for customer support agreements, comparisons of periodic operational performance reports with pre-determined operating goals, system incident reports, etc.

4.1.1.8.3 Determine whether the agency is maintaining unofficial or unauthorized ("cuff") records to fulfill their information needs because current systems are ineffective.

4.1.1.8.4 Identify deficiencies and ask users how the system could better support their needs.

4.1.1.8.5 Determine whether the agency has established problem management procedures. Obtain examples where operational problems have occurred and determine whether the problems (1) were resolved within the system or procedurally (i.e., a temporary workaround solution) and (2) caused any adverse effects on system operations, user satisfaction, or the attainment of program objectives.

4.1.1.8.6 Determine whether appropriate controls have been established to mitigate risks. For example, has the agency taken into account the feasibility or learning curve of moving from contractor-operated systems in the new environment to government-operated systems with individuals that have little or no experience in the new environment. Some of these individuals may have migrated over from the legacy system and its environment.

4.1.1.8.7 Verify the stability of the system support facilities. Addresses issues such as the adequacy of the power supply, air conditioning, humidity control.

4.1.1.8.8 Verify that the agency's continuity of operations plans are up-to-date and that they are periodically tested.

4.1.1.8.9 Evaluate that training programs adequately maintain skill levels for operations personnel.

4.1.1.8.10 Make a general assessment as to whether the agency is operating and managing day-to-day operations in compliance with policies, standards, procedures, and applicable laws and regulations.

4.1.1.9 Audit Products and Work Papers Developed in This Segment

4.1.1.9.1 Work papers that update and provide more details than the original agency profile.

4.1.1.9.2 Work papers summarizing the operational issues identified by the evaluation team.

4.1.2 System Measurement and Evaluation Segment

This segment focuses on measuring and evaluating overall system performance from several aspects. System performance involves factors such overall system responsiveness to the end user, availability, and reliability.

4.1.2.1 Agency Objectives for This Segment

4.1.2.1.1 Ensure that the agency has a systems management process in place that focuses on quantitatively measuring system performance from several standpoints, such as system responsiveness, availability, and reliability. This process should be supported by a quality assurance function that focuses on system stability as well as system improvement.

4.1.2.1.2 The agency should have a process that quantitatively gauges user and/or customer satisfaction.

4.1.2.1.3 Ensure that there is a process that periodically measures system cost effectiveness.

4.1.2.1.4 Ensure that agency personnel are properly trained and qualified to periodically measure and monitor system performance.

4.1.2.2 Relationship to Other Segments

During this segment the agency measures and evaluates how effectively, efficiently, and economically the system is operating to support the users' needs and the agency's mission.

4.1.2.3 Agency Products and Documents Delivered During This Segment

4.1.2.3.1 Routine and special monitoring reports of system performance produced for users, management, and IRM staff, including but not limited to:

a. trouble and downtime analysis reports;
b. on-time delivery reports/analysis;
c. on-time input receipt reports/analysis;
d. user satisfaction reports;
e. computer and communications equipment utilization statistics;
f. capacity planning updates.

4.1.2.4 Management Responsibilities Discharged in This Segment

4.1.2.4.1 Ensure that a computer performance management and network performance management process is in place and functioning effectively.

4.1.2.4.2 Ensure that agency personnel are properly trained to monitor and measure system performance.

4.1.2.4.3 Ensure that tools and techniques to measure system cost effectiveness, efficiency, and overall system performance are available and utilized.

4.1.2.4.4 Ensure that appropriate tests of management, environmental, and technical controls are planned and executed.

4.1.2.4.5 Monitor whether an effective security awareness program is operational and whether agency personnel are properly trained in matters relating to security.

4.1.2.4.6 Monitor whether a backup plan and contingency procedures are in place for continuity of operations and periodically tested.

4.1.2.5 User Responsibilities Discharged in This Segment

4.1.2.5.1 Monitor whether user information and service requirements are being met.

4.1.2.5.2 Work with IRM staff to plan and execute the tests of system controls as needed.

4.1.2.5.3 Work with IRM personnel to periodically assess vulnerabilities and threats to the system operating environment (e.g., user access codes, natural disasters, power loss)

4.1.2.6 IRM Responsibilities Discharged in This Segment

4.1.2.6.1 Work with users to determine whether user information and service requirements are being met. Obtain feedback from users on required improvements.

4.1.2.6.2 Measure and evaluate the level and quality of service provided to users and report on deviations, malfunctions, and other problems impacting user satisfaction.

4.1.2.6.3 Measure overall system responsiveness, availability, and reliability and analyze trends.

4.1.2.6.4 Perform workload measurement, characterization, and forecasting to predict future workloads and system characteristics.

4.1.2.6.5 Test disaster recovery plans and document the results.

4.1.2.6.6 Perform quality assurance to ensure that information products and services delivered are of high quality.

4.1.2.7 Audit Objectives During This Segment

4.1.2.7.1 Evaluate whether service-level agreements between users and IRM support staff are being fulfilled.

4.1.2.7.2 Verify that performance standards are being met.

4.1.2.7.3 Verify that controls are implemented to safeguard the systems and information resources against unauthorized use, accidental loss, fraud, waste, and abuse.

4.1.2.7.4 Verify the operational stability of the system by evaluating system responsiveness, availability, reliability, etc.

4.1.2.8 Audit Tasks for This Segment

4.1.2.8.1 Review service-level agreements between users and IRM support staff and verify that they are being fulfilled.

4.1.2.8.2 Verify that agency analyses of system responsiveness, availability, and reliability are accurate and complete.

4.1.2.8.3 Verify that the results of agency tests for continuity of operations are accurate and complete.

4.1.2.8.4 Verify that controls have been tested by the agency to ensure that (1) the system produces accurate, complete, reliable, and timely information to users and (2) the system is protected against unauthorized access, accidental loss, fraud, waste, abuse, and mismanagement.

4.1.2.8.5 Determine whether an effective security awareness program is operational and that agency personnel are properly trained in matters relating to security.

4.1.2.8.6 Verify that the agency is managing its operations in compliance with policies, standards, procedures, and applicable laws and regulations.

4.1.2.9 Audit Products and Work Papers Developed in This Segment

4.1.2.9.1 The following products should be collected from the agency:

a. trouble and downtime analysis reports;
b. on-time delivery reports/analysis;
c. on-time input receipt reports/analysis;
d. computer and communications equipment utilization statistics;
e. capacity planning updates; and
f. user satisfaction reports.

4.1.2.9.2 Work paper summaries documenting (1) the existence and adherence to service-level agreements between users and IRM support staff; (2) the verification of various agency system performance analyses (i.e., system responsiveness, availability, and reliability); (3) the verification of system cost-effectiveness studies; and (4) the evaluation team's analysis of overall system stability.

4.2 System Maintenance

The System Maintenance part begins after an initial operational capability (IOC) has been established and continues following full deployment of the system. In this part, the agency is primarily concerned with overall system stability and operational integrity. From an equipment perspective, there is preventive maintenance and remedial maintenance. From a software standpoint, there is remedial maintenance, minor modifications, and major modifications. Maintenance activities include (1) diagnosing conditions to identify opportunities to either avoid or lessen the impact of potential problems (i.e., preventive maintenance); (2) correction of hardware and software faults (corrective maintenance); and (3) adding new or replacement functions and features to the hardware or software (i.e., perfective and adaptive maintenance).

The system configuration for hardware and software is controlled typically by a configuration manager to ensure that the modifications to the system are (1) approved by management prior to implementation except for emergencies; (2) identified and tracked; and (3) limited to a small finite number of different versions and releases. Additionally, when emergency changes do occur, they are evaluated after the fact, adjusted if necessary, and formally approved by management.

Maintenance is a continuous activity that spans the entire useful life of the system. The total costs associated with maintaining systems over their life spans can often be significantly greater than that for developing or acquiring the system. Accordingly, information on the amount of maintenance necessary to keep the system operating effectively and efficiently provides feedback to the agency's information planning process. Extensive maintenance activities are often a basis for system replacement.

Preventive maintenance is an activity that is normally carried out by operations personnel and tends to apply to hardware and environmental units. Actions can include cleaning the heads of tape drives, cleaning removable disk units or changing filters on air conditioning units. The remaining categories of maintenance will be addressed in (1) the system configuration management segment, and (2) the system modification segment.

- System Configuration Management. The configuration management staff receives, classifies, evaluates, and prioritizes (1) system change requests (i.e., requests for modifications to the software or changes to the hardware configuration) and (2) system incident reports (i.e., sometimes referred to as trouble reports).

- System Modification. The maintenance staff designs the changes needed to modify or enhance the system, makes the changes, tests the changes on the system, and revises the system documentation.

Risk Management

The risk management plan should identify objectives and strategies that can be used to minimize the risk of failure during the maintenance process. For example, ease of maintenance could be an important objective for a system that is expected to receive a lot of changes over a relatively short period of time. A system that must react to changes in the tax law could be an example of this situation.

There should be a check and balance process in place that guarantees that management has complete visibility into the change control process. The changing of computer equipment, communications equipment, standard software, procedures, etc. should not occur without the knowledge and approval of the appropriate level of management. Similarly, the use of untested technology should not occur without management approval.

User development of local applications should not occur without the knowledge and approval of management. User changes to standard applications and COTS software should be discouraged.

Agency Profile

This part relies on the agency profile for information regarding the current IRM organization and standards, policies, and procedures. Past reviews, audits, or studies may direct the audit team to deficiencies related to system maintenance. System profiles provide insight into the current IRM environment.

4.2.1 System Configuration Management Segment

In this segment, the configuration management staff receives, classifies, evaluates, and prioritizes (1) system change requests (i.e., requests for modifications to the software or changes to the hardware configuration) and (2) system incident reports (sometimes referred to as trouble reports). The objective is to ensure (1) that desired changes to system functions, features, and operations are clearly controlled and documented and (2) overall system stability.

When system change requests are received they should be expediently classified, evaluated, and prioritized to ensure that changes that are critical to some defined operational objective (i.e., a change to preserve system responsiveness as a result of installing a new processor and operating system version, correction of a security weakness, adding a new application function, etc.) are acted upon first.

An analysis of the various classes of requested changes is required as a basis for priority-setting. Assignment of priorities to change requests must involve business as well as technical judgement. With the exception of emergencies, it is more prudent to establish a formal release schedule (monthly, quarterly, semi-annually, for example) for system changes than to continually change in an ad hoc manner.

Cost-benefit analysis is a key component in determining priorities. However, critical business or regulatory issues can override cost-benefit relative to priority setting. Some technical changes having limited cost-benefit, such as upgrading an operating system, may be required for continued satisfactory vendor support and be very high priority.

Finally, an implementation schedule is established and communicated to managers and users.

4.2.1.1 Agency Objectives for This Segment

- 4.2.1.1.1 Determine what changes to the system are required by system operators and users and document these as formal change requests.
- 4.2.1.1.2 Collect, log, and track all system change requests and communicate their status to users, management, and other appropriate parties.
- 4.2.1.1.3 Classify and evaluate all system change requests to assess their impact on the system.
- 4.2.1.1.4 Prioritize system change requests within classification groups (e.g., computer equipment, telecommunications, application software).

4.2.1.2 Relationship to Other Segments

In this segment, the configuration management staff receives, classifies, evaluates, and prioritizes system change requests and system incident reports.

4.2.1.3 Agency Products and Documents Delivered During This Segment

4.2.1.3.1 System incident reports (often known as trouble reports). These may generate a need for a system change request.

a. System change requests from operators or users.

b. System change request log that compiles and classifies the requests.

c. Reports to users and management communicating the status of their change requests.

4.2.1.4 Management Responsibilities Discharged in This Segment

4.2.1.4.1 Ensure that policies and procedures are in place that describe the system change control process including assignment of responsibilities, delegation of authority, and accountability.

4.2.1.4.2 Review and approve system change requests unless this authority has been delegated to a lower level.

4.2.1.4.3 Review priorities to ensure that they are consistent with organizational priorities.

4.2.1.4.4 Provide sufficient resources to facilitate user involvement and feedback on change request priorities.

4.2.1.4.5 Provide the resources necessary to analyze and estimate the effort of each system change request.

4.2.1.5 User Responsibilities Discharged in This Segment

4.2.1.5.1 Identify and report problems encountered in using the system (i.e., system incident reports).

4.2.1.5.2 Identify and report any newly desired or required functional or operational changes to the system (i.e., system change requests).

4.2.1.5.3 Articulate the urgency of requested or required system changes.

4.2.1.5.4 Work cooperatively with the maintenance and operations staff in the priority-setting process.

4.2.1.6 IRM Responsibilities Discharged in This Segment

4.2.1.6.1 Meet with management, user groups, and system operators on a regular basis to discuss changes that may be required for the system and maintenance policies and procedures.

4.2.1.6.2 Evaluate system change requests received from management, user groups, and system operators.

4.2.1.6.3 Maintain the change request log.

4.2.1.6.4 Regularly communicate the status of system change requests to users, system operators, and management.

4.2.1.6.5 Perform an initial impact analysis for each change request.

4.2.1.6.6 Derive an initial cost and schedule estimate to implement the system change request. This estimate, together with the mission-critical nature of the system change request, will help to determine its relative priority.

4.2.1.7 Audit Objectives During This Segment

4.2.1.7.1 Verify that agencywide policies and procedures for system change control exist.

4.2.1.7.2 Determine if a system change control process is being applied to the system under evaluation. Review the process used for consistency with agencywide policies and procedures.

4.2.1.7.3 Determine whether the change request logging process exists, and whether it formally and clearly establishes a history of change requests.

4.2.1.7.4 Evaluate the integrity of the change request classification process.

4.2.1.7.5 Evaluate the priority-setting process for creditable and consistent results.

4.2.1.7.6 Evaluate the effectiveness of communication between users, management, and the maintenance staff.

4.2.1.8 Audit Tasks for This Segment

4.2.1.8.1 Interview both agency and program management to obtain policies and procedures that cover system change control and their expectations regarding expected usage within the organization.

4.2.1.8.2 Review the policies and procedures to verify that the change control policies and procedures exist and are both internally consistent and consistent with other agency policies.

4.2.1.8.3 Evaluate current practices within system operations and the user organizations to determine the degree of consistency between these practices and current policy.

4.2.1.8.4 Review the change request log, if any, for completeness, existence of anomalies, and inconsistencies.

4.2.1.8.5 Confirm that system operations and user group change requests are formally received, logged, classified, and prioritized.

4.2.1.8.6 Determine the reasonableness of the process the agency used to estimate (1) cost and time to implement the changes logged and (2) the impact on the system.

4.2.1.8.7 Review the prioritization process, examining specific change requests and their assigned priorities. Determine whether anomalies and inconsistencies exist in the prioritization process.

4.2.1.8.8 Evaluate the reasonableness of priorities.

4.2.1.8.9 Interview users to determine whether they are satisfied with the priorities assigned to change requests.

4.2.1.8.10 Verify that the disposition of system change requests is communicated to the requesting individual or organizational entity.

4.2.1.9 Audit Products and Work Papers Developed in This Segment

4.2.1.9.1 Copies of system change control policies and procedures.

4.2.1.9.2 Copies of system change requests and related documents (i.e., system incident reports, malfunction incident reports, emergency change reports).

4.2.1.9.3 Evaluation team work papers that summarize the results of the tasks in the audit plan.

BLANK PAGE

4.2.2 System Modification Segment

In this segment the system change requests generated by users and system operations are implemented (i.e., planned, designed, developed, tested, and deployed). The component tasks of this segment are (1) complete the detailed design of the changes, (2) modify the system and application software as required and install replacement hardware, (3) update user manuals and support software (the help menu), (4) revise technical reference manuals, and (5) test changes to ensure that the functional and operational performance of the system has not been degraded. Finally, all system change requests that have been accepted for a particular updated version or release must follow the practices established in the system design, development, and deployment phase to enhance the likelihood of successfully updating the system.

4.2.2.1 Agency Objectives for This Segment

4.2.2.1.1 Implement the approved system change requests in accord with the system engineering discipline prescribed in the system design, development, and deployment phase.

4.2.2.2 Relationship to Other Segments

In this segment the maintenance staff designs the changes needed to modify or enhance the system, makes the changes, tests the changes on the system, and revises the system documentation.

4.2.2.3 Agency Products and Documents Delivered During This Segment

4.2.2.3.1 Plans (including deployment) and detailed analyses for the collective system changes.

4.2.2.3.2 System specifications for the design modifications and updated hardware configuration diagrams.

4.2.2.3.3 Revised software and the documented results of various tests (i.e., unit tests, integration tests, stress tests).

4.2.2.3.4 Test analysis report summarizing the results of a formal validation and verification test.

4.2.2.3.5 Updated technical documentation including programming segments and data dictionary.

4.2.2.3.6 Updated user documentation including procedures and training.

4.2.2.4 Management Responsibilities Discharged in This Segment

4.2.2.4.1 Provide the necessary resources to support the planning, analysis, design, development, and deployment of the approved system changes.

4.2.2.4.2 Ensure that the policies, procedures, and standards necessary to support system and software engineering practices is in place and enforced.

4.2.2.4.3 Manage to cost, schedule, and product quality objectives.

4.2.2.4.4 Ensure that approved system changes have been thoroughly tested including independent validation and verification prior to full deployment.

4.2.2.5 User Responsibilities Discharged in This Segment

4.2.2.5.1 Communicate with maintenance staff to determine the status of the project during this segment. If problems cause delays, users should be aware of reasons for such delay, and assist whenever possible to resolve issues that cause delays.

4.2.2.6 IRM Responsibilities Discharged in This Segment

4.2.2.6.1 Develop test data, test model, and document test conditions for unit testing as required.

4.2.2.6.2 Coordinate the testing of individual program modules and those that may have to interface with other modules (i.e., identify modules that raise integration issues).

4.2.2.6.3 Complete the detailed design, development and testing of software including independent validation and verification prior to deployment.

4.2.2.6.4 Ensure that changes to the hardware configuration and/or communications network are thoroughly tested prior to full deployment.

4.2.2.6.5 Document all changes to the detailed design specifications that may have been required during programming and testing of the software.

4.2.2.6.6 Assist with quality assurance as appropriate and ensure that system development standards are followed.

4.2.2.6.7 Inform management of potential problems that may cause delays in implementing major changes.

4.2.2.6.8 Plan the deployment of the change so as to minimize operational disruption. For example, include backup and recovery considerations in case the change does not work as planned.

4.2.2.7 Audit Objectives During This Segment

Determine whether the agency:

4.2.2.7.1 completed the detailed design;

4.2.2.7.2 implemented and documented the software and hardware changes;

4.2.2.7.3 verified that the changes are consistent with user requirements as expressed in the system change requests;

4.2.2.7.4 used system and software engineering practices including technical standards and tools in the system modification; and

4.2.2.7.5 used prudent management practices to minimize system maintenance.

4.2.2.8 Audit Tasks for This Segment

4.2.2.8.1 Review system change requests to determine if the disposition of the requests was determined in an expedient manner. Determine the role that priority setting played in this process.

4.2.2.8.2 Evaluate the adequacy of the system and software engineering practices used in implementing the approved changes.

4.2.2.8.3 Examine the technical standards and tools used in design and development such as software configuration management tools, reliability assessment models, and project management and system development software tools, and assess the quality of the system development environment.

4.2.2.8.4 Review the user documentation (procedures, manuals, on-line help, etc.) to determine whether this documentation clearly and accurately reflects the change request.

4.2.2.8.5 Interview QA personnel and users to verify that hardware and software changes were adequately tested using policies and procedures established by the agency.

4.2.2.8.6 Evaluate the agency's actual costs and schedule against the various estimates produced during the modification and inquire as to what adjustments the agency intends to make to its estimating process to improve in the future.

4.2.2.9 Audit Products and Work Papers Developed in This Segment

4.2.2.9.1 Work papers summarizing the evaluation team's analysis of the design, development, testing, and deployment process.

4.2.2.9.2 Evidence of support tools and standards that the agency used in doing the work in this segment.

4.2.2.9.3 Results of an assessment of the modification cost and schedule - actual versus planned.

Appendix A - Profile

The agency profile contains pertinent background information about the agency mission, organizational structure, programmatic goals and objectives, and extent to which it relies on information resource management activities. The agency profile is a prerequisite for most audit work. It provides the auditor with a basic understanding of the agency and its activities and will enable the auditor to deal with agency officials on an informed basis during all stages of the audit.

Agency profiles can be developed on an entire department or agency, or a unit or bureau within the department or agency, whichever is appropriate for the audit. Where key decisions are made with respect to the system being audited is the determining factor for deciding what profile information should be gathered. For example, if key decisions are being made at the Department level, then the profile should be developed at that level.

An agency profile will be prepared on all audits and Issue Areas Director have already prepared profiles for many agency AIS. Consequently, it may only be necessary to update a previously developed agency profile for retention as part of the permanent audit site files for future use. Therefore, the agency profile is the basis for the audit work plan. The audit staff should begin at the audit site by requesting updates to files or copies of agency information gathered in earlier audits. Having obtained all available information regarding updates to relevant information that may have been collected earlier, the audit staff should include a list of outstanding data or information requests with the agency notification letter, requesting that copies of the needed information be given to the audit staff prior to the opening conference. Once the information is received, it should be reviewed so that any clarifications can be obtained at the opening conference or initial interviews.

As a general rule, agency profiles will contain information on missions, goals, and objectives; agency organization and responsibilities; information resources management (IRM) organization and responsibilities; standards, policies, and procedures; internal and external audits, reviews, and studies; systems inventories; and past and current problems. Each of these major categories is discussed in detail below.

Missions, Goals, and Objectives

Agencies need information to achieve their mission, goals, and objectives. To understand why an agency defines its information needs the way it does and how it manages its information resources to meet these needs, it is important to have a working knowledge of the agency's mission, goals, and objectives.

This working knowledge comes from two sets of documents. One set includes legislation, legislative histories, annual reports, and public relations material, and provides information on what the agency is trying to accomplish. These documents reveal what the Congress has said about the agency's mission, goals, and objectives and how the agency has interpreted the guidance the Congress has given it. The other set of documents which complements these documents, includes recent budgets and agency plans. These give a more dynamic picture of how the agency has been attempting to achieve its goals and objectives and what it is planning for the future.

In reviewing these documents, auditors should become familiar not only with the broad mission of the agency but also with the goals and objectives of the programs and activities that are designed to support the overall mission. Auditors will need to exercise judgment regarding how detailed an understanding of the agency's goals, objectives, and programs they should develop. During the survey phase, it will usually not be necessary to understand in complete detail how each program or activity is executed; however, it is important to understand how major programs are designed to accomplish their objectives in order to comfortably discuss agency information, activities, and programs later in the audit. When the audit enters the review phase, and the auditor must assess the effect of information resource management problems on agency goals and objectives, a more detailed understanding will usually be required.

Information to be Obtained

- Copies of pertinent bills, acts, titles, or laws pertaining to the agency.
- Copies of any legislative history that is necessary to explain how the agency is to implement legislation.
- Copies of documents in which the agency has stated and/or interpreted its mission, goals, and objectives, including:
  - annual report to the Congress,
  - recent congressional hearings on agency programs, and
  - public relations material, including pamphlets, brochures, newsletters, etc.
- Copies of the proposed budget, the current budget, and the budgets for the last 3 years for major programs and automated systems that support the agency's mission.
- Copies of planning documents, such as the strategic IRM plan, that address the development, and acquisition of major agency information systems.

Agency Organization and Responsibilities

Linked to a working knowledge of the agency's mission, goals, and objectives should be a working knowledge of how the agency is organized and where authority and responsibility are placed within the organization. By reviewing an agency's organizational documents and its budget and planning documents, the auditor can develop this working knowledge.

The agency should be organized in a way that supports the efficient, effective, and economical accomplishment of its missions, goals, and objectives. The organizational structure should reflect current operating conditions at the agency and should clearly delineate the roles, responsibilities, and relationships of organizational units. Within the organizational units, each individual should have clearly defined roles, responsibilities, and duties. Information management and technology functions should be organized and necessary responsibilities and functions delegated in a way that supports the agency's overall mission.

The agency's organization must be analyzed to identify potential weaknesses that could affect its information management and technology activities. The roles, responsibilities, and duties of individuals within the agency must be analyzed from the same perspective. Identified weaknesses can be translated into risks. For example, does the organizational structure inhibit the integration of information resource management, user management, and top management, or is the information management and technology function inappropriately placed within the agency? Are there cultural or political barriers to implementing efficient organizational structures? Any weaknesses (deficiencies) and risks identified should be documented and specifically addressed in the agency profile.

Information to be Obtained

-- A copy of the organization chart for the agency and its relevant components (i.e, subordinate departments, administrations, bureaus, divisions, etc.). The chart should identify key agency officials and include their titles, work locations, and telephone numbers.

-- A copy of the organization manual for agency and relevant components, which describes the responsibilities of the components and the key agency officials.

IRM Organization and Responsibilities

Having developed a working knowledge of the agency's mission, goals, and objectives and how it has organized itself to achieve these goals and objectives, the auditor now needs to understand how the agency is organized to meet its information needs and manage its information resources. In reviewing the documents obtained from the agency, the auditor should start with the senior IRM official and determine his location in the organization and his authority and responsibilities. In large agencies this official will typically perform only

top-level planning, policy setting, and evaluation, and will not be involved in the day-to-day management of information resources. Consequently, the auditor should work down to the level at which information resources are used and managed.

In identifying organizational elements where information resources are used and managed, the auditor should be alert to the variety of titles these elements might have, such as "Data Systems Division" or "Computer Service Center." The auditor should also be alert for situations where information resources are managed outside the formal IRM organization. For example, the purchase of word processors might be under the procurement office and therefore not be subject to policies established by the IRM organization regarding interconnection or compatibility.

Once organization elements are identified, the auditor should review pertinent documents that describe activities, authorities, and responsibilities of IRM staff.

Information to be Obtained

-- A copy of the organization chart for the senior IRM official's office and for any other IRM activities located throughout the organization. (Other IRM activities include, for example, automated data processing and/or computer centers that are under components of the agency or the telecommunications control center.)

-- A copy of the organization manual for the agency's IRM activities. If not available, substitute the position descriptions of the officials responsible for the various IRM activities.

-- A copy of position descriptions for determining the knowledge, skills, and abilities needed to accomplish IRM activities (e.g., systems development).

-- A copy of the staffing profile (positions filled and employee backgrounds) to compare against position descriptions.

Standards, Policies, and Procedures

The agency should have well established standards, policies, and procedures for carrying out its missions, goals, and objectives. Standards, policies, and procedures serve as a basis for management actions and provide criteria upon which to evaluate the activities resulting from those actions. Standards and policies are incorporated in the following compliance documents (a comprehensive list is contained in appendix C of this manual):

Statutory -- Computer Security Act, Brooks Act of 1965, Paperwork Reduction Act, etc.

Regulatory -- Office of Management and Budget Circulars, GAO Standards for Internal Controls, Federal Information Resources Management Regulation, etc.

Agency Directives -- Department of Defense Directive No. 8120.1, entitled Life Cycle Management of Automated Information Systems, National Security Decision Directive 145, entitled National Policy on Telecommunications and Automated Information Systems Security, etc.

Discretionary -- Federal Information Processing Standards Publication (FIPS Pub) 38, Guidelines for Documentation of Computer Programs and Automated Data Systems, FIPS Pub 49, Guidelines on Computer Performance Management: An Introduction, etc.

Agency policy directives define how the standards and policies are to be interpreted and implemented at the agency. Procedures describe the manner in which the policies are to be applied within the various agency components. Standards, policies, and procedures should be continuously updated and communicated to all affected organizational elements.

The extent to which the agency has (1) incorporated the standards promulgated by other authorities into its standards, policies, and procedures; (2) established policies that define the relationship between standards and agency implementation activities; and (3) developed procedures which describe the manner in which the policies are to be applied must be analyzed to identify potential weaknesses that could affect the agency's information management and technology activities. These weaknesses should then be translated into risks associated with the efficient, effective, and economical operation of the agency's automated systems. For example, is an agency in non-compliance with the Computer Security Act of 1987 due to inappropriate provisions in their implementing regulations caused in part by confusion with National Security Decision Directive 145 (NSDD-145)? Deficiencies, weaknesses, and risks identified should be documented and specifically addressed in the agency profile.

Information to be Obtained

-- Copies of pertinent standards that affect the agency's major programs and automated systems.

-- Copies of pertinent policies affecting the agency's major programs and automated systems.

-- Copies of pertinent procedures affecting the agency's major programs and automated systems.

Internal and External Audits, Reviews, and Studies

Audits, reviews, and studies are essential management tools. They are performed by internal organizational units (internal audit, quality assurance, security, end users, etc.), and external organizations (certified public accounting firms, consultants, GAO, etc.). Management should use these audits, reviews, and studies as appraisals of agency operations, complimenting other elements of management control. Management has, of course, a responsibility to see that appropriate corrective actions are taken on the recommendations resulting from these audits, reviews, and studies.

The extent to which the agency takes advantage of these management tools and uses them to take corrective actions must be analyzed to identify potential weaknesses that could affect the agency's information management and technology activities. These weaknesses can then be translated into risks associated with the efficient, effective, and economical operation of the agency's automated systems. For example, does the agency fail to take action on information management and technology deficiencies that contribute to material weaknesses identified by internal and external oversight, review or audit organizations? Deficiencies, weaknesses, and risks identified should be documented and specifically addressed in the agency profile.

Audits, reviews, and studies are very valuable resources for the auditor. They provide extensive information about past agency problems, and, if applicable to the current audit, should be used in assignment scoping and planning.

Information to be Obtained

- Copies of internal audits completed during the last 3 years dealing with information or information resource management problems.
- Summary of ongoing and planned internal audits dealing with information or information resource management problems.
- Copies of relevant GAO or Inspector General reports on agency information or information resources management problems. Include any reports on governmentwide information issues that refer to the agency being audited.
- Copies of contractor or consultant studies of the agency's information resources or information resources management activities.
- Copies of congressional testimony or reports of congressional hearings in which the agency's information resource management activities have been examined.

System Profile

A list of the agency's major automated information systems (AIS) and non-major systems that are relevant to the audit. Major AIS are defined in the amended version of OMB Circular A-130. Since many agencies have AIS that are poorly documented and not clearly defined, it is very important that special emphasis be placed on identifying those AIS that represent significant agency investments.

Information to be Obtained

- Copies of the current AIS strategic and tactical information management plans.
- Descriptions of existing performance measures for both the systems and programmatic areas used to deliver agency services or produce agency products.
- List of contact points of system employees with knowledge in the identified system.
- Description of the hardware platform (i.e., make and model), communication facilities (i.e., suppliers, makes, models) and executive and support software (i.e., language compiler version and release, DBMS version and release, operating system version and release, etc.).
- List and description of all relevant application systems including interfaces to other application systems.
- List and description of all relevant databases and files.

See the system profile worksheet at the end of this appendix for a more detailed list of information categories.

Past and Current Problems

The final step in the agency profile is to develop an overview of past and current problems regarding information resources management activities. Past problems can be identified by reviewing and summarizing completed audits, reviews, and studies. Current problems can be identified from several sources. The most obvious one is the GAO audit staff at the agency. Because of their considerable knowledge about the agency and its problems, the audit staff is likely to be aware of programs for which information needs are not being met, or instances where information resources are not being used efficiently and economically. Another source will be the agency's internal audit staff. Like GAO staff, their day-to-day presence at the agency gives them an intimate familiarity with the agency's programs and potential problem areas.

Budget and planning documents can also provide clues regarding problems the agency is trying to correct by indicating where the agency is allocating resources or plans to allocate resources. For example, the agency may be planning to expend significant resources on designing a new system in order to correct chronic problems with an existing system. These documents might also indicate potential problems by revealing, for example, a sharp cutback in automated data processing training expenditures. In addition, prior year copies of Federal Manager's Financial Integrity Act of 1982 reports covering internal control system weaknesses will also provide insight into agency problem areas and systems.

In categorizing the problems, auditors should try to distinguish between (1) those caused by the information not meeting identified needs and therefore impairing program effectiveness and (2) those caused by information resources not being used efficiently or economically. It is also important to relate problems to the agency's organizational structure so that chronic trouble spots can be identified.

Preparing the Profile

The purpose of the agency profile is to compile and document key agency data so that audit staff have a general understanding of the agency, its mission, and its operations. In addition, past and current problems at the agency and the extent of agency corrective actions should be documented in the agency profile. In many cases, the existing profile maintained by the Issue Areas Directors will be updated. However, in other cases, a profile will have to be developed.

The agency profile should be maintained as part of the permanent audit site files and should include the documents obtained and a brief summary of the information obtained for each of the categories: missions, goals, and objectives; agency organization and responsibilities; IRM organization and responsibilities; standards, policies, and procedures; internal and external audits, reviews, and studies; and past and current problems.

System Profile Worksheet		
System name		
Category	Examples	Comments/notes
Initiative program	Such as modernization, reengineering, technology update	
Contacts	Such as users, IRM, management	
System function	Business goals addressed by system	
	Business processes affected by system	
Background system history	Past problems, system being replaced, deployment history	
Stakeholders of system	Such as users, developers, vendors, contractors	
Financial information	Funding source	
	Life cycle costs	
	Annual operating costs	
	Relevant acquisitions	
	Relevant leases/contracts	
	Outsourcing agreements	
Location(s) of system	Data center name(s), geographic location, # sites, # users	
System attributes	Performance dimensions	
	Security certification	
	Expected system life	
Relationship to other systems/initiatives	Data sharing	
	Interfaces	
	Infrastructure usage	
	Dependencies	
	Architectures	
Applicable standards	External	
	Internal	
System components	Subsystems, modules	
Inputs/outputs	Such as report types, data entry mechanisms, GUIs	
Data processing now	Online/batch/real-time	
System structure	Centralized/distributed/client-server	
Processing load	Transaction types, frequency, CPU, program	
Configuration (include version, release, model and manufacturer for both hardware & software, commercial off the shelf or custom)	CPU type, model, manufacturer, data response	
	Storage devices	
	Peripheral devices	
	Operating system	
	Security software	
	Utilities	
	Other system software such as middleware, transaction processing monitors	
	Database management system	
	Network environment (include topology, protocols)	
	Application programs	
	Configuration management tools	
System development	Stage of development	
	Start date of development	
	End date (could be estimate)	
	Development methodologies used	
	Composition of development team	
	Development platform(s)	
	Programming language(s) used	
	CMM assessment of development group	

BLANK PAGE

Appendix B - Related Methodologies and Models

Federal Information System Controls Audit Manual (Exposure Draft) (GAO/AIMD January 1996).

Information Technology: An Audit Guide for Assessing Acquisition Risks (GAO/IMTEC 8.1.4, December 1992).

Information Technology: A Model to Help Managers Decrease Acquisition Risks (GAO/IMTEC 8.1.6, August 1990).

Strategic Information Planning: Framework for Designing and Developing System Architectures (GAO/IMTEC-92-51, June 1992).

Federal Financial Management Systems Review Methodology, Version 1.0 (GAO/AIMD December 1995).

Business Process Reengineering Assessment Guide, Version 3.0 (GAO/AIMD-10.1.15 April 1997).

Assessing Risks and Returns: A guide for Evaluating Federal Agencies' IT Investment Decision-making, Version 1.0 (GAO/AIMD-10.1.13 February 1997).

Strategic Information Management (SIM) Self-Assessment Toolkit (Exposure Draft), Version 1.0, (GAO/AIMD October 1994).

Government Auditing Standards: 1994 Revision (GAO/OCG-94-4, June 1994).

A Systems Engineering Capability Maturity Model, Version 1.1, Software Engineering Institute, November 1995.

The Program Manager's Guide to Software Acquisition Best Practices, DoD Software Acquisition Best Practices Initiative, September 1995.

Software Capability Evaluation Method Description, Version 2.0, Software Engineering Institute, June 1994.

Capability Maturity Model for Software, Version 1.1, Software Engineering Institute, Feburary 1993.

BLANK PAGE

Appendix C - Applicable Criteria

Short title	Criteria description	1.0 Planning		2.0 Concept	3.0 Design, Development & Deployment		4.0 Operations & Maintenance	
		1.1 Strategic Planning	1.2 Program Planning	2.1 Concept Exploration	3.1 Iterative DOD	3.2 Custom DOD	4.1 Ops	4.2 Maint
DOD Standard 2168-1979	Military Standard: Defense System Software Quality Program			X	X	X	X	X
IEEE Standard 982.2-1988	Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software				X	X	X	X
IEEE Standard 983-1986	Guide for Software Quality Assurance Planning		X		X			
IEEE Standard 1016-1987	Recommended Practice for Software Design Descriptions				X	X		
IEEE Standard 1028-1988	Standard for Software Reviews and Audits		X		X	X		X
IEEE Standard 1042-1987	Guide to Software Configuration Management		X		X	X	X	X
IEEE Standard 1058.1-1987	Standard for Software Project Management Plans		X	X				
ISO 9000-3-1991	Quality Management and Quality Assurance Standards - Part 3: Guidelines for the Application of ISO 9001 to the Development, Supply and Maintenance of Software				X	X		X
DOD 499b	Systems Engineering, MIL-STD-499b			X	X	X		
DOD 498	Software Development and Documentation, MIL-STD-498		X		X	X		X
DOD5200.28	Trusted Computer System Evaluation Criteria, DOD Standard 5200.28		X			X	X	X
DOD8000.1	Defense Information Management Program, DOD Directive 8000.1	X	X					
DOD8120.1	Life Cycle Management of AISs, DOD Directive 8120.1, January 14, 1993		X	X	X	X		
FAR	Federal Acquisition Regulation (FAR), General Services Administration				X	X		
FIPS 38	Guidelines for Documentation of Computer Programs and Automated Data Systems		X		X	X	X	X
FIPS 65	Guideline for Automatic Data Processing Risk Analysis, FIPS Pub 65, National Institute of Standards and Technology, August 1, 1979		X	X				
FIPS 73	Guidelines for Security of Computer Applications, FIPS PUB 73, National Institute of Standards and Technology, June 30, 1980		X		X	X		

Short title	Criteria description	1.0 Planning		2.0 Concept	3.0 Design, Development & Deployment		4.0 Operations & Maintenance	
		1.1 Strategic Planning	1.2 Program Planning	2.1 Concept & Project Initiation	3.1 Iterative D/D/D	3.2 Custom D/D/D	4.1 Ops	4.2 Maint
FIPS 87	Guidelines for ADP Contingency Planning, FIPS PUB 87, National Institute of Standards and Technology, March 27, 1981.				X	X		
FIPS101	Guideline for Lifecycle Validation, Verification, and Testing of Computer Software, FIPS PUB 101, National Institute of Standards and Technology, June 6, 1983.				X	X		
FIPS102	Guidelines for Computer Security Certification and Accreditation, FIPS PUB 102, National Institute of Standards and Technology, September 27, 1983.				X	X	X	
FIPS105	Guidelines for Software Documentation Management, FIPS Pub 105, National Institute of Standards and Technology, June 6, 1984.		X		X	X	X	X
FIPS106	Guideline on Software Maintenance, FIPS PUB 106, National Institute of Standards and Technology, June 15, 1984.						X	X
FIPS110	Guideline for Choosing a Data Management Approach, FIPS PUB 110, National Institute of Standards and Technology, December 11, 1984.			X	X	X		
FIPS123	Specification for a Data Descriptive File for Information Interchange (DDI) (ANSI/ISO 8211-1985), FIPS PUB 123, National Institute of Standards and Technology, September 19, 1988.				X	X		
FIPS132	Guideline for Software Verification and Validation Plans (ANSI/IEEE 1012-1986), FIPS PUB 132, National Institute of Standards and Technology, November 19, 1987.				X	X		
FIRMR	Federal Information Resources Management Regulation (FIRMR), General Services Administration.	X	X	X	X	X	X	X
GAO	Information Technology: A Model to Help Managers Decrease Acquisition Risks				X	X		
GAO-51	Strategic Information Planning - Framework for Designing and Developing System Architectures, GAO/IMTEC-92-51	X	X	X				
GSA81-2	Conversion Contracting Techniques Associated with Procurement of a Replacement ADP Hardware System, General Services Administration, September 1981.				X	X		
GSA82-2	Conversion Work Packages, General Services Administration, July 1982.				X	X		
GSA83-1	Conversion Plan Outline, General Services Administration, January 1983.				X	X		

Short title	Criteria description	1.0 Planning		2.0 Concept	3.0 Design, Development & Deployment		4.0 Operations & Maintenance	
		1.1 Strategic Planning	1.2 Program Planning	2.1 Concept Exploration	3.1 Iterative DDD	3.2 Custom DDD	4.1 Ops	4.2 Maint
GSA83-2	Software Conversion Lessons Learned, Volume I, General Services Administration, January 1983.				X	X		
GSA83-3	Guidelines for Planning and Implementing a Software Improvement Program (SIP), General Services Administration, May 1983.	X	X					
GSA84-1	Preparing Software Conversion Studies, General Services Administration, January 1984.				X	X		
GSA84-2	Software Tool Evaluation and Selection Guidelines, General Services Administration, August 1984.				X	X		
GSA85	Software Aids and Tools Survey, General Services Administration, November 1985.				X	X		
GSA88-1	Conversion Cost Model (Version 4), General Services Administration, May 1988.				X	X		
GSA88-2	Programmers Workbench Handbook, General Services Administration, June 1988.				X	X		
GSA66-3	Information Systems Planning Handbook, General Services Administration, December 1986.	X	X	X				
GSACFR1	ADP Management Programs, 41 CFR 201-20, General Services Administration.	X	X	X				
GSACFR2	Contracting for ADP Resources., 41 CFR 201-32, General Services Administration.				X	X		
GSACFR3	Requirements Analysis, 41 CFR 210-20.003, General Services Administration.				X	X		
IEEE 730	Software Quality Assurance Plans, ANSI/IEEE Standard 730-1989			X	X	X		X
IEEE 828	Standard for Software Configuration Management Plans, ANSI/IEEE Std 828-1983.				X	X		X
IEEE 829	Software Test Documentation, ANSI/IEEE Standard 829-1983				X	X		X
IEEE 830	Guide to Software Requirements Specifications, ANSI/IEEE Standard 830-1984				X	X		
IEEE 982.1	Standard Dictionary of Measures to Produce Reliable Software, IEEE Standard 982.1-1988				X	X		
IEEE 982.2	Guide for Use of IEEE Standard Dictionary of Measures to Produce Reliable Software, IEEE Standard 982.2-1988				X	X		X
IEEE 983	Guide for Software Quality Assurance Planning, IEEE Standard 983-1986				X			X
IEEE1008	Software Unit Testing, IEEE Standard 1008-1987				X	X		X

Short title	Criteria description	1.0 Planning		2.0 Concept	3.0 Design, Development & Deployment		4.0 Operations & Maintenance	
		1.1 Strategic Planning	1.2 Program Planning	2.1 Concept & Project Initiation	3.1 Iterative DD/D	3.2 Custom DD/D	4.1 Ops	4.2 Maint.
IEEE1012	Software Verification and Validation Plans, IEEE Standard 1012-1986				X	X		X
IEEE1016	Recommended Practice for Software Design Descriptions, IEEE Standard 1016-1987				X	X		X
IEEE1028	Standard for Software Review and Audits, IEEE Standard 1028-1988				X	X	X	X
IEEE1042	Guide to Software Configuration Management, IEEE Standard 1042-1987				X	X	X	
IEEE1058.1	Standard for Software Project Management Plans, IEEE Standard 1058.1-1987			X				
IEEE1074	Developing Software Life Cycle Processes, Project Management Processes, PreDevelopment Processes and Development Processes, IEEE Standard 1074-1991		X	X	X	X	X	X
ISO 9000-3	Quality management and quality assurance standards for the application of ISO 9001 to the development, supply, and maintenance of software, ISO 9000-3			X	X	X		X
NBS500-98	Planning for Software Validation, Verification, and Testing, Edited by Patricia B. Powell, NBS Special Publication 500-98, National Institute of Standards and Technology, November 1982				X	X		
NBS 500-105	Guide to Software Conversion Management, Edited by M. Skall, NBS Special Publication 500-105, National Institute of Standards and Technology, October 1983				X	X		
NBS 500-133	Technology Assessment - Methods for Measuring the Levels of Computer Security, William Neugent, John Gilligan, Lance Hoffman, Zella G. Ruthberg, NBS Special Publication 500-133, National Institute of Standards and Technology, October 1985						X	
NBS 500-136	An Overview of Computer Software Acceptance Testing, Dolores R. Wallace, NBS Special Publication 500-136, National Institute of Standards and Technology, February 19, 1988				X	X		
NIST500-180	Guide to Software Acceptance, Dolores R. Wallace, John C. Chamarsky, NIST Special Publication 500-180, National Institute of Standards and Technology, April 1990				X	X		
OMB A-123r	Internal Control Systems, OMB Circular A-123 Revised, Office of Management and Budget, August 16, 1983	X	X	X	X	X	X	X
OMB A-127	Financial Management Systems, OMB Circular A-127, Office of Management and Budget, December 19, 1984		X	X	X	X	X	X

Short title	Criteria description	1.0 Planning		2.0 Concept	3.0 Design, Development & Deployment		4.0 Operations & Maintenance	
		1.1 Strategic Planning	1.2 Program Planning	2.1 Concept &Project Initiation	3.1 Iterative DDD	3.2 Custom DDD	4.1 Ops	4.2 Maint
OMB A-130	Management of Federal Information Resources, Office of Management and Budget, Circular A-130		X		X	X	X	X
PL96-511	Paperwork Reduction Act of 1980, 44 U.S.C. 3501, Public Law 96-511, December 11, 1980	X	X	X				
GPRA	Government Performance and Results Act, 5 U.S.C. 306, NLT 9/30/97	X					X	
CMM	Capability Maturity Model for Software, Version 1.1 (CMU/SEI-93-TR-24), Software Engineering Institute, February 1993				X	X	X	X
CMM-SE	A System Engineering Capability Maturity Model, Version 1.1 (CMU/SEI-95-MM-003), Software Engineering Institute, November 1995		X	X	X	X		
SABP	A Program Manager's Guide to Software Acquisition Best Practices, Version 1.1, DoD Software Acquisition Best Practices Initiative, September 1995				X	X		

BLANK PAGE

Appendix D - SAF Quick Reference

Each of the following pages corresponds to a specific SAF part and its segments. On each page is a table that summarizes the agency's system life cycle activities and the agency's responsibilities for that part.

Segment	1.1.1 Scope, Definition, and Organization	1.1.2 Status and Opportunity	1.1.3 IRM Strategy
Objectives of the segment	Obtain executive-level management commitment, involvement, control, and accountability for the business and strategic IRM planning process. Develop a business plan. Establish & organize the strategic IRM planning process. Assign leadership and staff responsibilities. Define the scope, objectives, and approach. Provide training to steering committee and planning team.	Understand the forces of the external environment. Identify the agency's missions, goals, and objectives. Estimate IRM performance for probable future scenarios. Document major information technological and functional trends. Define major IRM objectives to satisfy information needs in support of agency mission, goals, and objectives.	Develop high-level IRM strategy reflecting a 5-7 year, agencywide view, and (b) any budgetary constraints. Produce an IRM strategic plan. Obtain management review and approval of the IRM strategy and strategic plan.
Products and documents delivered during the segment	Business plan. Charter. Documentation of key mission and program planning issues to be resolved/addressed during the IRM strategic planning process. Work program or other documentation describing the schedule of planning milestones and management checkpoints.	Description of external factors that influence or constrain the agency's planning process. Description of the agency's missions, goals, and objectives. Analysis of agency management, program operations, overall agency performance in light of probable future scenarios. Analysis of the impact and causes of any weaknesses. Description and assessment of IRM infrastructure to support probable future scenarios. Description of information technology and functional trends. Summary of major IRM objectives.	IRM strategic plan that provides at minimum, a 5-7 year projection of major functions and operations of the agency.
Management's responsibilities	Commitment to and involvement with the planning process. Appoint IRM planning team members and define the charter and responsibilities of those involved. Define key mission and program planning issues, performance measures, management concerns, and expectations. Provide the planning team with leadership. Review and approve the schedule of planning milestones and management checkpoints.	Provide a vision of the agency's probable future scenarios. Identify IRM objectives. Provide guidance to help the planning team assess current conditions and identify opportunities for improvement. Help the planning team define the strategic management information needed. Review results of status and opportunity assessment and provide consensus or approval.	Provide final executive-level comments, guidance, suggestions, and constructive criticism to help the planning team complete the IRM strategy and strategic plan. Ensure that the IRM strategic plan is consistent with and linked to the agency business plan. Review and approve the IRM strategy and strategic plan.
User's responsibilities	Identify specific high-level members to participate on the planning team. Work with IRM staff to define strategic program-related issues to be addressed during the planning process.	Assist the planning team in identifying (1) the strengths and weaknesses of programmatic operations and constituents' satisfaction with agency performance, (2) strengths and weaknesses of existing technological capabilities, and (3) the IRM objectives for supporting the agency's strategic vision. Assist team in assessing the current IRM infrastructure.	Assist the planning team in formulating proposed IRM strategies and developing the strategic plan. Assist the planning team in presenting the proposed strategies and plan to management.
IRM's responsibilities	Identify specific high-level members to participate on the planning team. Work with users to help define strategic program-related issues to be addressed during the planning process.	Assist the planning team in assessing (1) the current IRM infrastructure and its potential capability for supporting the agency's vision, and (2) the IRM objectives for supporting the agency's strategic vision. Be alert to trends, and identify new technologies that may be applied in support of the agency's vision.	Assist the planning team in formulating proposed IRM strategies and developing the strategic plan. Assist the planning team in presenting the proposed strategies and plan to management.

Segment	1.2.1 Scope, Definition, and Organization	1.2.2 Status and Opportunity	1.2.3 IRM Strategy
Objectives of the segment	Obtain program management's commitment, involvement, control, and accountability for the planning process. Establish and organize IRM operational planning. Define the scope, objectives, and approach. Identify issues that will shape or affect the IRM operational plan. Provide necessary training. Plan a quality assurance and system configuration management process.	Understand the forces of the external environment. Determine the impact and causes of any weaknesses. Assess satisfaction with existing information systems, services, and products and establish measures of performance. Identify ways to better use information resources. Identify the information products, services, and resources needed to support program goals and objectives effectively and efficiently. Assess current IRM technical support operations, technical architecture, and capacity. Assess the skills, practices, and organization of the IRM community. Assess technology trends and identify opportunities for using new technology. Define major IRM objectives. The	Develop an implementation strategy for inclusion in the IRM operational plan. Produce an IRM operational plan that will describe how IRM resources will be used to support program goals and objectives. Obtain management review and approval of the IRM operational plan.
Products and documents delivered during the segment	Charter for the program planning team. A listing of key mission and program planning issues to be addressed. Work program including schedule of planning milestones and management checkpoints.	Description of the agency's missions, goals, objectives, and external environment. Analysis of the impact and causes of any weaknesses or deficiencies. Description and assessment of user/customer satisfaction. Description of new ways and approaches to better use information technology. Description of information products, services, and resources needed. Analysis of current IRM technical support operations, technical architecture, and capacity. Description and assessment of IRM organization. Description of major information technology trends. Definition of criteria for establishing priorities among systems development projects.	IRM operational plan. Preliminary cost-benefit analysis and/or alternatives analysis for each major project summarized in the operational plan. Preliminary IRM budget for each major project summarized in the operational plan.
Management's responsibilities	Commitment to and involvement in the planning process. Appoint IRM planning team members and define the charter and responsibilities of those involved. Define key mission and program planning issues and performance measures, as well as key management concerns and expectations. Review and approve the planning schedule and work program.	Provide a clear statement of the agency's mission, goals, and objectives. Provide the planning team with inputs from program managers, including priority setting criteria, guidance, suggestions, and constructive criticism. Identify and communicate to the planning team the management information needed to manage program operations and activities, including information needed to measure program performance. Review results of status and opportunity assessment and provide consensus or approval before the planning team begins work on the next segment.	Provide final comments to help the planning team complete the IRM implementation strategy and operational plan. Ensure that the IRM operational plan is consistent with and linked to the IRM strategic and agency business plans. Review and approve the IRM implementation strategy and operational plan.
Users' responsibilities	Identify specific members to participate on the planning team. Work with IRM staff to define program-level operational issues to be addressed during the planning process.	Assist the planning team in identifying (1) strengths and weaknesses of existing technological capabilities, and (2) the information products, systems, and services needed to accomplish program goals and objectives and satisfy customer needs. Identify extent to which current systems and functional processes meet user needs, and identify opportunities for work process re-design and improving program operations. Assist the planning team in assessing the skills, practices, and organization of user groups.	Assist the planning team in formulating the IRM implementation strategy and developing the operational plan. Assist the planning team in presenting the proposed strategies and plan to program management.
IRM's responsibilities	Identify specific members to participate on the planning team. Work with users to help define program-level operational issues to be addressed during the planning process.	Assist the planning team in identifying current status of and potential improvements to program applications of information technology, and identify opportunities for work process redesign and improving program operations. Be alert to trends and identify new technologies that may be applied in support of agency operations. Assist the planning team to define major information technology objectives. Assist the planning team in assessing the IRM community.	Assist the planning team in formulating the IRM implementation strategy and developing the operational plan. Assist the planning team in presenting the proposed strategies and plan to program management.

Segment	2.1.1 Project Initiation	2.1.2 Project Definition	2.1.3 Work Plan, Standards, and Project Organization	2.1.4 Management Review and Approval
Objectives for the segment	Approve initiation Select project teams	Define scope of project Select architecture concept Select transition or development approach Estimate costs Perform cost-benefit, feasibility, & risk analyses. Identify project constraints	Develop project work plan or work breakdown structure Establish appropriate controls Adopt and/or develop standards Develop an organizational structure for completing the project.	Ensure that the project will correct existing deficiencies Ensure that performance goal can be met Ensure that the user and IRM organizations agree with the project team's proposal Obtain authorization to proceed to D/D/D phase
Products and documents delivered during the segment	Authorization request. Project team charter.	Deficiencies to be addressed Alternative approaches. System concept. Cost-benefit analyses. Approximate life cycle costs. Technical feasibility study. Risk Management Analysis.	Work plan. Project Standards. Organizational Structure.	Project team report. System concept Work plan. Adopted standards Organizational structure Management approval
Management's responsibilities	Review proposal. Approve/reject decision.	Ensure that all work done by project team is validated by users. Ensure that project satisfies identified needs.	Ensure user and IRM coordination. Review and approve the work plan, project standards, and organization structure.	Review the project team report. Ensure that service or performance goals will be met. Authorize proceeding to D/D/D phase.
Users' responsibilities	Commit appropriate personnel to project team.	Review and validate concept of operations. Approve project scope and system concept.	Work with project team to identify and commit personnel with appropriate skills for design and development.	Collaborate with the project team in preparing the report and obtaining management approval.
IRM's responsibilities	Commit personnel to project team.	Provide support for: scoping the project, developing system concept, preparing C/B analyses, risk management analysis, technical feasibility study, and life cycle cost estimates.	Provide support for: developing work plan, adopting appropriate standards, selecting project management tools, defining the org structure and project resource requirements, obtaining user agreement on work plan, project standards, and org structure.	Provide support for: preparing the report and obtaining user's concurrence, and submitting the report to management for approval

Segment	3.1.1 Needs Identification and Design	3.1.2 System Development and Deployment	3.1.3 Review
Objectives of this segment	Identify specific requirements Prepare, review, and release an RFP for competitive bids Ensure communication between users and developers Describe and document the existing system's input, output, and processing functions, if applicable Determine and define the iterative approach to be taken Examine system architectural alternatives Develop a work plan, test plan, transition policies & procedures Establish appropriate computing resources Prepare estimated project costs Develop or update risk management plan Verify and validate all analyses and plans that are developed Resolve open issues regarding major requirements	Reconfirm requirements. Reevaluate alternatives Complete the detailed design, if necessary Develop the code and the test plans Revise the initial estimates for cost, schedule, level of effort, and computing resource requirements Ensure that all interfaces have been identified Continue to reiterate design, coding, and testing until users are satisfied and accept the system Obtain management approval Install the system at an initial operational site Update and review risk analyses	Review the results of a formal CITR. If the system does not satisfy user needs, decide whether to continue developing the system using the same iterative approach (next cycle), a new strategy, or abandon the system Review and compare cost and schedule estimates to actual expenditures Ensure that communication channels to users remain open Review and approve the RFP or other solicitation request, if applicable
Products and documents delivered during this segment	High-level user requirements. Overview of the current system. System functional requirements. Work plan, approved project request. Description of alternative technical solutions. Updated cost-benefit analyses, risk analyses. Design of QA & CM processes. Project status reports. Records of meetings with users & management. RFP, if appropriate.	Completed system or subsystem Detailed design document Program documentation and code listings Verification and validation of test plans & results Integration charts or diagrams, where appropriate Evidence of "walk-throughs" and acceptance Records of change requests, meetings, status reports Updated work plan, economic analyses & risk analyses Request for mgmt approval of all design iterations RFP or other solicitation document, if appropriate.	Summary and analysis of experience gained in this segment Records of user acceptance and a decision to proceed to the operations and maintenance phase, or evidence of additional enhancements and a decision to continue reiterating, or evidence of a decision to abandon the project RFP (if appropriate)
Management's responsibilities	Approve the scope of the iteration being developed. If contractual support is needed, approve the solicitation. Review cost and risk analyses. Require that IRM and user organizations work together. Ensure that the required computing resources are available. Review the products and deliverables. Authorize proceeding with this iteration. Monitor the project's progress using the defined QA process.	Reconfirm scope of the project. Ensure that IRM and user organizations coordinate on test results and system changes. Ensure that the products from this segment meet the agency's mission and satisfy user requirements. Monitor progress of the project.	Decide whether to accept the system as operational, abandon it, or continue. Reconfirm that IRM and user organizations are effectively coordinating. Provide the funding and resources. Approve the proposed schedule. If management decides to stop the project, then authorize abandoning the project.
Users' responsibilities	Identify and define requirements. Specify performance, security, and integrity requirements. Ensure that personnel with appropriate skills are available. Participate with IRM staff to select a particular iterative method. Participate with IRM staff to design and document the system. Work with the IRM staff to update alternative analyses. Verify and validate system requirements.	Reconfirm requirements and ensure that requirements are met. Work with the IRM organization to update economic and technical alternatives. Inform management of changes to the user organization that may result from using the system.	Decide whether the entire system or part of the system meets requirements. Decide whether to proceed with subsequent iterative cycles to more closely meet actual functional and operational requirements.
IRM's responsibilities	With user participation, develop system functional requirements, system specifications, updated technical alternatives, economic analyses, risk analyses & the overall iteration approach. Work with appropriate users to design and document the system. Prepare a request for approval to proceed with development. Prepare and present progress reports to management. Prepare and advertise solicitation document, if appropriate. Implement the quality assurance and control plan. Develop & implement a configuration management process. Ensure that policies and procedures are established for transitioning to the new system.	Create and update all technical documentation. Incrementally and iteratively develop code, test, and install the proposed system. Review and update technical alternative approaches to satisfy user needs. Update economic and risk analyses. Update established procedures for manual and automated processes. Prepare and present progress reports to management.	Confirm that completed iterations meet user requirements. Continue to present progress reports to management. If development is to continue, work with users to refine system functions, features & operational characteristics. Define and document "lessons learned." Complete all relevant system documentation.

Segment	3.2.1 Needs Identification	3.2.2 System Design	3.2.3 System Development and Deployment
Objectives of the segment	Identify, define, and document specific user requirements Define deliverables Develop and review policies and procedures that will support the transition to the new system Obtain management approval for the user requirements	Define inputs and outputs to the system, processing functions, overall system architecture, and constraints Develop the system design specification If appropriate, develop a solicitation document Approval of the system design specification Convert functional specs to application program specs Analyze the feasibility of the system design Identify the human interfaces to the system & the procedures required to support these interfaces Estimate training needs	Translate the system design specifications into computer software Establish and implement an SQA function Develop and implement test plans Ensure that an IV&V of the system is conducted Ensure that user acceptance tests are conducted Place approved products under configuration control Ensure that the system is still affordable and cost-effective Develop and implement a transition strategy Develop and obtain approval for a solicitation document if necessary Develop and implement acquisition plans, and installation plans
Products and documents delivered during the segment	High-level user requirements Overview of the current or proposed system System functional requirements Project status reports Records of meetings between users IRM & management Approved request document A solicitation document, if contractual support is required	System design specifications Project status reports Minutes of meetings Relevant project approval documents A solicitation document, if required Technical architecture Logical and physical database design specifications Software development strategy Performance expectations	Organization charts. Applicable policies, procedures, and standards Completed work plan. Programming specifications Program development and test library Test analysis report Library of production quality application software System support documentation.Training schedule & course materials Transition plan, deployment plan, Continuity of operations plan and procedures. Telecom network management plan, if applicable Performance measures that link to the users' operations
Management's responsibilities	Authorize proceeding with the segment. Develop or update a risk management plan. Review and approve user requirements. Develop a solicitation document, if necessary, and ensure that IRM, contractors (if used) and users work together Ensure that products generated in the segment are consistent with the agency's objectives, support tools and the computing environment needed are available, project costs are within goals, and project milestones are being met.	Approve strategy for system development and installation. Ensure use of agency-accepted policies, methods, standards and tools Provide the resources and skill levels needed Review and approve the overall system. Monitor progress of the project. Review and approve proposed service levels required by user Review and approve the approach for security, data integrity, and application controls	Review and approve the development approach, system test and conversion plans, transition plan, training plan, requests for changes to system requirements, and formal releases of the system Monitor critical aspects of contractor development activity, if applicable Conduct progress reviews and approve required adjustments. Establish performance measures Ensure that quality assurance and appropriate standards have been implemented, that the appropriate SW engineering environment is in place, and that formal verification and validation occurs Agreement that acceptance test results meet management's criteria Conduct formal milestone
Users' responsibilities	Participate with the IRM group to develop and present the proposed functional and operational requirements to management for approval. Specify performance, security, data integrity, and reliability control requirements Ensure that personnel with appropriate business and functional skills are available Review and approve the business area analysis or the required operational capability	Work with IRM to further clarify system requirements Review and concur with the system design specifications. Define required system performance, service levels, security, data integrity, and audit trail control requirements. Assist IRM in evaluating technical architecture options and tradeoffs Assist IRM in defining all interfaces to the system.	Participate in verification & validation of system functions Ensure user participation during implementation and installation Work with IRM staff develop system support products & training plan Define system test conditions, and test data Assist the IRM staff in the development of the overall transition strategy and plan, in the review and control of system change requests, and in the verification of system test results Participate with IRM staff in acceptance Assist the IRM staff in collecting information on system costs incurred and benefits realized.
IRM's responsibilities	Work with users to identify and define user requirements and system functional specs. Develop, with user assistance, internal controls, system characteristics & features, procedures for manual & automated processes, and any database, network or telecom requirements. Prepare and present progress and status reports to management. Develop and obtain approval for a solicitation document for contractual support if necessary Formally coordinate with users	Work with users to refine system specifications and user processing needs. Develop the solicitation document and obtain approval, if applicable Present progress reports to management. Ensure the integrity of the system design specs. Follow defined methodologies, if in place Prepare the technical architecture specification. Determine network topology and design the network. Design database structures. Design the application programs. Develop preliminary test plans. Update the risk analysis.	Work with the users to develop the solicitation document and obtain management approval, if necessary Develop detailed design specifications and test and conversion plans Develop the applications software Test the program modules Install system software and hardware as necessary Document changes to the detailed design specs, code & procedures Assist management with overall quality assurance Inform management of potential problems Ensure that the development team has the needed skills Develop a deployment plan

Segment	4.1.1 Day-to-Day Operations	4.1.2 System Measurement and Evaluation Segment
Objectives for the segment	Implement operating plans Ensure that budgets allow for day-to-day operations Ensure that policies and procedures for input and output are being implemented Manage facility operations, telecommunications resources Coordinate with maintenance staff to update system resource components as required Provide support to and users in a controlled environment Manage and implement security policies and procedures Provide training for operations personnel	Have a systems management process in place Quantitatively gauge user or customer satisfaction Periodically measure system cost effectiveness Ensure that agency personnel are properly trained and qualified to periodically measure and monitor system performance
Products and documents delivered during this segment	Updated and current operations and procedures manuals Periodic risk analyses Periodic budget, cost-benefit, and operational performance analyses Periodic performance indicators and trends	Routine and special monitoring reports of system performance, such as - trouble and downtime analysis reports - on-time delivery reports/analysis - on-time input receipt reports/analysis - user satisfaction reports - computer and communications equipment utilization statistics - capacity planning updates
Management's responsibilities	Ensure that resources are available to operate the system. Manage the resources committed to or used in operating the system. Ensure that a security awareness program is operational. Ensure that internal controls are established and followed. Manage exceptions to standard operating procedures and the use of standard products. Ensure that IRM unit is satisfying user needs. Ensure that end-user applications conform to plans, budgets, internal controls, policies, standards, and procedures. Review and approve updates to operating plans, budgets, policies, standards, and procedures. Ensure that agency personnel are properly trained to operate the system, and in security. Ensure that IRM and users agree to changes in technology, and that such changes are introduced in a controlled manner.	Ensure that a computer performance management and network performance management process is in place and functioning effectively. Ensure that agency personnel are properly trained to monitor and measure system performance. Ensure that tools and techniques to measure system cost effectiveness, efficiency, and overall system performance are available and utilized. Ensure that appropriate tests of management, environmental, and technical controls are planned and executed. Monitor security awareness and training. Monitor whether a backup plan and contingency procedures are in place for continuity of operations and periodically tested.
Users' responsibilities	Establish operating plans and procedures for implementing their missions. Establish work performance agreements with IRM. Utilize resources in an effective, economical, and efficient manner. Maintain and manage information that supports the agency's mission, program objectives, and policies. Work with IRM to ensure that information and system services are complete, accurate, reliable, secure, and timely. Submit input data in accordance with published schedules and established operating procedures. Verify the results of processing. Grant access to programs and data on a need-to-use basis and report access violations to the security administrator.	Monitor whether user information and service requirements are being met. Work with IRM staff to plan and execute the tests of system controls as needed. Work with IRM personnel to periodically assess the vulnerabilities and threats to the system operating environment.
IRM's responsibilities	Operate and control systems resources. Schedule and monitor automated information system support activities. Provide users with necessary information products and services. Identify and resolve environmental problems that affect operations and communicate these to management. Control the media library and the movement and usage of storage media. Ensure system availability, reliability, responsiveness, etc. Ensure continuity of operations. Identify alternative and new technologies that can be applied to improve operational effectiveness.	Work with users to determine whether user information and service requirements are being met. Obtain feedback from users on required improvements. Measure and evaluate the level and quality of service provided to users and report on problems affecting user satisfaction. Measure overall system responsiveness, availability, and reliability and analyze trends. Perform workload measurement, characterization, and forecasting to predict future workloads and system characteristics. Test disaster recovery plans and document the results. Perform quality assurance.

Segment	4.2.1 System Configuration Management	4.2.2 System Modification
Objectives for the segment	Determine what changes to the system are required by system operators and users, and document these as formal change requests. Collect, log, and track all system change requests and communicate their status to users, management, and other appropriate parties. Classify and evaluate all system change requests. Prioritize system change requests within classification groups.	Implement the approved system change requests in accord with the system engineering discipline prescribed in the system design, development, and deployment phase.
Products and documents delivered during this segment	System incident reports. System change requests from operators or users. System change request log that compiles and classifies the requests. Reports to users and management communicating the status of their change requests.	Plans and detailed analyses for the collective system changes. System specifications for the design modifications and updated hardware configuration diagrams. Revised software and the documented results of various tests. Test analysis report summarizing the results of a formal validation and verification test. Updated technical documentation including programming segments and data dictionary. Updated user documentation including procedures and training.
Management's responsibilities	Ensure that policies and procedures are in place that describe the system change control process including assignment of responsibilities, delegation of authority, and accountability. Review and approve system change requests unless this authority has been delegated to a lower level. Review priorities to ensure that they are consistent with organizational priorities. Provide sufficient resources to facilitate user involvement and feedback on change request priorities. Provide the resources necessary to analyze and estimate the effort of each system change request.	Provide the necessary resources to support the planning, analysis, design, development, and deployment of the approved system changes. Ensure that the policies, procedures, and standards necessary to support system and software engineering practices is in place and enforced. Manage to cost, schedule, and product quality objectives. Ensure that approved system changes have been thoroughly tested, including independent validation and verification prior to full deployment.
Users' responsibilities	Identify and report problems encountered in using the system. Identify and report any newly desired or required functional or operational changes to the system. Articulate the urgency of requested or required system changes. Work cooperatively with the maintenance and operations staff in the priority-setting process.	Communicate with maintenance staff to determine the status of the project during this segment. If problems cause delays, users should be aware of reasons for such delays and assist whenever possible to resolve issues that cause delays.
IRM's responsibilities	Meet with management, user groups, and system operators on a regular basis to discuss changes that may be required for the system, and maintenance policies and procedures. Evaluate system change requests received from management, user groups, and system operators. Maintain the change request log. Regularly communicate the status of system change requests to users, system operators, and management. Perform an initial impact analysis for each change request. Derive an initial cost and schedule estimate to implement the system change request.	Develop test data, test model, and document test conditions for unit testing as required. Coordinate the testing of individual program modules and those that may have to interface with other modules. Complete the detailed design, development, and testing of software including independent validation and verification prior to deployment. Ensure that changes to the hardware configuration or communications network are thoroughly tested prior to full deployment. Document all changes to the detailed design specifications that may have been initiated during programming and testing of the software. Assist with quality assurance, as appropriate, and ensure that system development standards are followed. Inform management of potential problems that may cause delays in implementing major changes. Plan the deployment of the change so as to minimize operational disruption.

Appendix E - Submitting Comments

Feedback on this manual is encouraged. Please use the following forms or their equivalent

SAF Change Request - for specific changes.

SAF Comment Form - for general comments

Post-Assignment Survey - to describe how SAF was used during an assignment

GAO DCA users will be able to edit electronic versions of these forms.

Written comments should be sent to the following address:

U.S. General Accounting Office
Accounting and Information Management Division
Room 4S10
441 G St. NW
Washington, D.C. 20548

Attn: Paul Silverman, Project Manager

Comments may also be sent by email to the following address:

silvermanp.aimd@gao.gov

SAF Change Request

Name/Title	Phone:
Organization Mailing Address:	Email:
	Date:

Type (check one)			Would you like a reply? (check one)		
		High Priority Change Request			Yes
		Low Priority Change Request			No

Applicable SAF Section(s):

Change Description (if specifying additional criteria or methodology information, please include the version number, date, and source):

Please print or write below the line

Action:	Date:

SAF Comments

Name/Title:	Phone:		
Organization/Mailing Address:	Email:		
	Date:		
	Would you like a reply? (check one)		Yes
			No
Applicable SAF Section(s):			
Accuracy:			
Organization:			
Completeness:			
Ease of Use:			
Other: Please don't write below this line			
Action:	Date:		

Post-Assignment Survey

Name/Title/Job Series:	Phone:
Organization/Mailing Address:	Email:
	Date:

Assignment Objective:	Job Code

How did you use SAF in your assignment? (check all that apply)

- ☐ As criteria
- ☐ As a reference to other criteria
- ☐ As a reference to other methodologies
- ☐ As a technical reference
- ☐ As a checklist
- ☐ Other:

When did you use SAF in your assignment? (check all that apply)

- ☐ Planning assignments
- ☐ Staffing the assignment team
- ☐ Preparing the work plan
- ☐ Collecting data
- ☐ Analyzing data
- ☐ Message agreement
- ☐ Report Writing
- ☐ Other:

Which sections of SAF did you find the most useful?

Which sections of SAF did you find least useful?

What other methodologies/guidance did you use in your assignment?

Which best describes SAF? ☐ Too technical ☐ About right ☐ Not technical enough

Other comments:

Please don't write below this line

Action:	Date:

Glossary

Acceptance Test	A formal evaluation performed by a customer to verify that the manufacturer has met the agreed-upon specifications and that a device is functioning as intended.
Access	The ability and the means necessary to approach, input, or retrieve data or software, and/or communicate with, or make use of any resource of an automated information system.
Access Control	Ensuring that the resources of an AIS can be accessed only by authorized users in authorized ways.
Access Control Mechanism	Hardware or software features operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access to an automated data processing system.
Access Method	The technique used to access data on a physical file device. Types of access methods include sequential, index sequential, hierarchical structure, network structure, and relational structure.
Access Methods	A method of transferring data between the computer's main storage and an input/output device.
Accountability	The ability to hold individuals responsible for their actions.
Accreditation	The managerial authorization and approval, granted to an AIS system or network, to process sensitive data in an operational environment, made on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet pre-specified technical requirements for achieving adequate data security. Management can accredit a system at a higher/lower level than the certification. If management accredits the system at a higher level than it is certified, management is accepting the residual risk (difference between the levels of accreditation and certification).
Accuracy	Information that is free of error. [Small acceptable errors in an AIS can still be considered accurate.] Synonymous with integrity.

Acquisition	The obtaining, by contract with appropriated funds, of supplies or services (including construction) by and for the use of the federal government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract.
Acquisition Planning	The process by which the efforts of all personnel responsible for an acquisition are coordinated and integrated through a comprehensive plan for fulfilling the agency need in a timely manner and at a reasonable cost. It includes developing the overall strategy for managing the acquisition.
Administrative Procedure	A detailed set of human processable operating instructions required to accomplish a specific process within a sub-system. Administrative procedures detail manual steps along with explanations and examples. Procedures used for such things as performing routine or clerical assignments, making decisions, report distribution, input preparation, or for using "office automation" related equipment.
Administrative Security [Controls]	The management constraints and supplemental controls (rules and procedures) established to provide an acceptable level of protection for data. Synonymous with procedural security.
ADP	Abbreviation for automated data processing
Agency Procurement Request (APR)	A request by a federal agency for the General Services Agency to acquire information processing resources or delegate the authority to acquire these resources.
AIS	Abbreviation for automated information system
AIS Assets	The components of an AIS, including hardware, software, data, and people.
Algorithm	A prescribed set of well-defined rules for the solution of a problem in a finite number of steps. Generally, a complex formula for solving a specific mathematical problem.
Analysis	A major phase of the systems life cycle, synonymous with planning.

Application	A computer program designed to help people perform a certain type of work. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements.
Application Controls	Methods and procedures designed for each application (contained in application software) to ensure the authority of data origination, the accuracy of data input, integrity of processing, and verification and distribution of output.
Application Software	Computer programs that perform data processing functions rather than control functions.
Applications Software	There are two types of software: applications software and systems software. Both are written in computer languages and can be called programs. Applications software is software that does something for the user. Anybody who uses the computer is called a user.
Architecture	A description of all functional activities to be performed to achieve the desired mission, the system elements needed to perform the functions, and the designation of performance levels of those system elements. An architecture also includes information on the technologies, interfaces, and location of functions and is considered an evolving description of an approach to achieving a desired mission.
Artificial Intelligence (AI)	The branch of computer science that deals with enabling computers to emulate such aspects of intelligence as speech recognition, deduction, inference, creative response, the ability to learn from past experience, and the ability to make reasonable inferences from incomplete information.
Audit Trail	The chronological set of records that provides evidence of system activity. These records can be used to reconstruct, review, and examine transactions from inception to output of final results. The records can also be used to track system usage and detect and identify intruders.
Audit [security-related use of term]	To record independently and later examine (selected security relevant) system activity.

Auditability	Relates to the production and retention, by an AIS, of a record of significant processing events that affect security along with the ability to locate and reconstruct those events. Auditability also encompasses the system of internal controls that ensures the integrity of processing and the protection of the audit records.
Authentication	1. Verification of the identity of a user or the user's eligibility to access an AIS. 2. Verification that a message has not been altered or corrupted.
Authorization	The right granted to an individual to use the system and the data stored on it.
Authorization	1. A user's right to communicate with or make use of a computer system. 2. An access right. 3. The process of granting a user either complete or restricted access to an AIS resource or function.
Automated Information System (AIS)	An automated system for the organized collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures.
Automated Systems Engineering (ASE)	A software tool used to automatically design an information system and the application logical database. Unlike CASE tools, ASE's orientation is on total system design, not just software, and systems integration through shared data.
Automatic Data Processing (ADP)	Information processed by computers. Also used to refer to computer resources.
Automatic Data Processing Equipment (ADPE)	ADP equipment is equipment used in support of an organization's information environment, consisting of computer and telecommunications hardware and their related components.
Availability	A timing consideration for specifying how and when data is collected from various sources within an enterprise. Availability answers the question, "Is the data there when I need it?" How data is made available is a function of input.

Awareness Training

Mandatory periodic training required by the Computer Security Act of 1987 for all employees who are involved with the management, use, or operation of federal computer systems. Awareness training creates a sensitivity to threats and vulnerabilities and the recognition of the need to protect data, information, and the means of processing them.

Backup

A duplicate copy of a program, disk, or data made either for archiving purposes or for safeguarding valuable files from loss should the active copy be damaged or destroyed.

Backup Procedure

1. The provisions made in a contingency plan for the recovery of data and for restart or replacement of computer hardware and software after a system failure or disaster.

2. Copying of data to a medium from which the data can be restored if the original data is destroyed or compromised. Full backups copy all data in the system. Incremental backups copy only data that's been changed since the last full backup. A sound backup plan involves keeping backup media off-site and developing procedures for replacing system components, if necessary, after a system failure.

Baseline

A specification or product that has been formally reviewed and agreed upon that thereafter serves as the basis for further development and that can be changed only through formal change control procedures.

Baseline Architecture

The initial architecture that is or can be used as a starting point for subsequent architectures or to measure progress.

Benchmark

A set of computer programs and associated data tailored to represent a particular work load and used to evaluate system performance or cost. A benchmark test is a user-witnessed demonstration on a vendor's proposed computer system, done to validate system performance or cost. Benchmark tests are needed to assess how a vendor's system will process the work load (e.g., processing speed, resource consumption) and to compare the performance of several systems.

Benchmark Test

A test that uses a representative set of programs and data designed to evaluate the performance of computer hardware and software in a given configuration.

Best and Final Offer	A final opportunity for offerors in the competitive range to revise proposals.
Blueprinting	The process of producing a consistent set of codable, physical plans for construction.
Bottom-up Programming	A programming technique in which lower-level functions are developed and tested first; higher-level functions are then built using the lower-level functions and so on.
Bottom-Up Design Method	Forming and layering groups of instruction sequences together, starting at a machine instructional level and working up to a complete solution.
Break Even Point	A point in time where cost savings match accumulated development expenses.
Basic Telecommunications Access Method (BTAM)	An IBM abbreviation for Basic Telecommunications Access Method, a software protocol used to control the transfer of data between main storage and local or remote terminals. BTAM provides the macro instructions for utilizing the capabilities of the devices supported. Used in binary synchronous as well as start/stop communications.
Budgeting and Costing	Budgeting, often considered to be part of the short-term planning function, establishes financial and other targets and commitments based on the best plans possible and supported with as much quantitative and qualitative data as are available. Budgeting also represents a primary form of control over actual actions and expenditures because these are compared with those budgeted (planned). Budgets, as an element of both planning and control, require and involve analyses, explanations, and justifications. They are also used for evaluation of significant deviations. These deviations and their causes should be considered in developing future plans and budgets.
Bundled	A pricing strategy in which a computer manufacturer includes all products -- hardware, software, services, training, etc., in a single price.

Business Plan	An action plan that the enterprise will follow on a short-term and/or long-term basis. It specifies the strategic and tactical objectives of the company over a period of time. The plan, therefore, is time dependent; it will change with the enterprise. Although a business plan is usually written in a style unique to a specific enterprise, it should concisely describe what is planned, why it is planned, when it will be implemented, by who, and how it will be gauged. The architects of the plan are typically the principals of the enterprise.
Business Process Re-Engineering (BPR)	BPR is the total redesign of the functions performed in carrying out an organization's mission, using advanced technology as an enabler. The redesign tackles problems in today's business processes: (1) too much time and money spent coordinating and communicating and too little time doing work that benefits customers and (2) boundaries between departments representing barriers to change.
CAD/CAM	Computer-Aided Design/Computer-Aided Manufacturing.
Canard	A wrong-headed assumption about some subject.
Capability Validation	The technical verification of the ability of a proposed system configuration, replacement component, or the features or functions of its software, to satisfy functional requirements. The intent is to ensure that the proposed resources can provide the required functions.
Capacity	The amount of information a computer or an attached device can process or store.
Capacity Management	Involves analyzing the performance of computer systems and forecasting computer resource (hardware) requirements to ensure sufficient capacity exists when needed.
Capacity Management Activities	Include collecting and analyzing detailed performance (system utilization) data on current computer processing and comprehensive modeling and pilot testing of planned computer systems. Such activities must also include characterization of the work load in units that will allow comparison to the system's processing capabilities.
CASE	A comprehensive label for software designed to use computers in all phases of computer program development.

CASE (Computer Aided Software Engineering)	Automated tools that provide support for software engineering activities. They should not be confused as tools for Systems Engineering; their perspective is on software engineering only.
CASE tools	Computer-Aided Software Engineering (CASE) tools.
Certification	1. A written guarantee that a system or component complies with its specified requirements and is acceptable for operational use. For example, a written authorization that a computer system is secure and is permitted to operate in a defined environment. 2. A formal demonstration that a system or component complies with its specified requirements and is acceptable for operational use. 3. The process of confirming that a system or component complies with its specified requirements and is acceptable for operational use.
Certification (and accreditation)	The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a prespecified set of security requirements.
Chief Information Officer (CIO)	An executive-level officer who represents the chief information broker/architect/strategist of a company. The CIO reports to the Chief Executive Officer (CEO) and maintains a lateral working relationship with the Chief Operating Officer (COO) and Chief Financial Officer (CFO).
Client/Server Architecture	An arrangement used on local area networks that makes use of "distributed intelligence" to treat both the server and the individual workstations as intelligent programmable devices, thus exploiting the full computing power of each.
Closed Architecture	A term used to describe any computer design whose specifications are not freely available.

Closed Shop	The operation of a computer facility where programming service to the user is the responsibility of a group of specialists, thereby effectively separating the phase of task formulation from that of computer implementation. The programmers are not allowed in the computer room to run or oversee the running of their programs. Contrasted with Open Shop.
COBOL	Common Business Oriented Language. A data processing language for computer programming that makes use of English language statements. It is especially adapted to business and commercial problems.
Code	A system of symbols and rules for use in representing information.
Code Conversion	The conversion of data from one code to another.
Coding	Creating the software used by the computer from program flowcharts.
Cohesion	The measure of the inner strength or relatedness of the various elements of a module. Functional modules have the highest cohesion.
Cold Site	An alternative (computer or communications) facility with the equipment necessary to support the installation and operation of a computer center in the event of a disaster such as flood or fire. (Usually does not include any computer equipment.) Contrast with hot site.
Command, Control, and Communications (CCC)	CCC is a term used primarily in the defense industry to represent an information system.
Commerce Business Daily	A daily publication that lists the government's procurement invitations, contract awards, subcontracting leads, sales, surplus property, and foreign business opportunities.
Communication Protocol	A set of rules that govern communications among computer systems. Standard protocols, when implemented, allow different manufacturers' computer systems to communicate.
Communications	The transmission of data or information from one place or piece of equipment--a computer, for example--to another.
Compartment	A non-hierarchical designation applied to sensitive information in one or more categories to denote special handling and access control restrictions.

Compatibility	The characteristic of data processing equipment by which one machine may accept and process data prepared by another machine without conversion or code modification.
Compatibility-Limited Requirement	A statement of requirements expressed in terms that require items to be compatible with existing information processing resources.
Competitive Range	The group of offerors selected, after technical and cost evaluation, to whom award of a contract is a reasonable possibility.
Completeness Check	A survey to determine that all data required in a record is present.
Component	A single resource with defined characteristics. The component concept is used for defining precise specifications for the various resources for testing their validity. These components are also defined by their relationship to other components.
Compromise	A violation of the security system such that an unauthorized disclosure, modification, or destruction of sensitive information may have occurred or that a denial of service condition has been induced.
Computer	A device capable of solving problems or manipulating data by accepting data, performing prescribed operations on the data, and supplying the results of these operations. Various types of computers are: analog, digital and calculator.
Computer Aided Design (CAD)	Computer software/hardware that is used to assist in the logical and physical design of a product. In IRM terms, CAD is implemented using Automated Systems Engineering (ASE), prototyping aids, and documentation aids.
Computer Aided Manufacturing (CAM)	Computer software/hardware that is used to assist in the manufacturing of a product. In IRM terms, CAM is implemented using fourth generation languages, program generators, report writers, job control language generators, data description language generators, etc.
Computer, Fixed Program	A computer in which the sequence of instructions are permanently stored or wired in and perform automatically and are not subject to change either by the computer or the programmer except by rewiring or changing the storage input.

Computer fraud	A computer crime that involves deliberate misrepresentation or alteration of data and/or software in order to obtain something of value, usually for monetary gain.
Computer Languages, Syntax	People communicate with computers via the artificial computer languages in which programs are written. The instructions that make up a program consist of a series of statements arranged according to the syntax (a set of rules, like grammar, governing instructions and parameters) of the language.
Computer Program	A set of instructions in some computer language intended to be executed on a computer to perform a useful task.
Computer Security	Concepts and techniques (physical, administrative, and technical measures) used to protect the hardware, software, and data of an AIS from deliberate or inadvertent damage, destruction, disclosure, manipulation, modification, use, or loss. The objectives of computer security are to ensure system integrity and availability and information confidentiality.
Computer Software	Machine processable instructions for operating a specific computer. There are two aspects to computer software: system software which is concerned with the basic operational needs required to operate computer hardware (i.e., operating systems, communication utilities, performance monitors, editors, compilers, etc.), and application software, which is concerned with having the computer perform specialized tasks to assist users in their effort.
Computer, Stored Program	A digital computer that under control of its own instructions, can synthesize, alter, and store instructions as though they were data and can subsequently execute these new instructions.
Concurrency	The logical relationship between two or more actions or data that can occur at the same time.
Concurrent	A term applied to a computer operation in which two or more processes (programs) have access to the microprocessor's time and are therefore carried out more or less at the same time.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Configuration	A group of machines that are interconnected and are programmed to operate as a system.
Configuration Control	An element of configuration management consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification.
Configuration Item	An aggregation of hardware and/or software that is designated for configuration management and treated as a single entity in the configuration management process.
Configuration Management (control)	The identification, control, accounting, and auditing of all changes to system hardware, software, firmware, documentation, test plans, and test results throughout the development and operation of the system.
Configuration Management	The continuous control of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system.
Consistency Check	A survey to determine that items of data conform to certain formats, bounds, and other parameters and are not internally contradictory.
Construction	A major phase of the systems life cycle. It constitutes the process of coding, compiling, assembling, and testing a system from a physical systems design.
Contingency Plan	A plan for responding to the loss of system use due to a disaster such as a flood, fire, or computer virus. The plan contains procedures for emergency response, backup, and post-disaster recovery.
Continuity of Operations	A system architecture that provides ADP availability within a predefined time period after system failure as measured by the restart/recovery time (for example, continuous for redundant components, 30 milliseconds, 30 minutes, or 30 hours). (The major security risks during the continuity of operations process include bypassing security controls during restart/recovery operations.)
Contracting Officer (CO)	A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

Contracting Officer's Technical Representative (COTR)

An individual to whom the CO delegates certain contract responsibilities, usually related to technical acceptance issues.

Control Objectives

The internal control goals or targets that management tries to achieve or negative effects that management seeks to avoid for each type of transaction.

Control Program

The program responsible for handling input/output for both terminals and file storage, establishing processing priorities, maintaining waiting lists of work in process, activating operational programs, and performing other supervisory functions in a real-time system. Words sometimes used synonymously to designate such a program include driver, executive, monitor, and supervisor.

Controlling

Controlling can be considered the function designed to close the management loop. Many controls are designed to:

1. provide timely feedback on how well organizational plans are being executed;
2. identify problems, their significance, and causes; and
3. give management a basis for establishing priorities to correct problems so that operations are productive, run economically, efficiently, and effectively, and support organizational missions, goals, and objectives.

Conversion

1. The process of changing information from one form of representation to another, such as from the language of one type of machine to that of another or from magnetic tape to the printed page. Synonymous with data conversion.
2. The process of changing from one data processing method to another, or from one type of equipment to another; e.g., conversion from punch card equipment to magnetic tape equipment.

Cost/Benefit Analysis

An analysis of the costs or expenses incurred by a project in comparison to the benefits derived from implementing the project. This analysis is also used to determine the value of information.

Cost-Reimbursement Contract	A contract in which the government reimburses the contractor for expenses so long a the contractor provides its "best effort" to complete the work called for.
Central Processing Unit (CPU)	The heart of the general purpose computer that controls the interpretation and execution of instructions. Does not include interface, main memory, or peripherals. It also controls input and output units and auxiliary attachments.
Critical Path	The longest path in a project methodology that is critical to the timely completion of a project or part of a project. A project always has a critical path until it is completed or canceled. The path may vary according to accomplishments.
Criticality	The importance of the information to enable an agency to accomplish its mission. Includes the importance of the mission itself.
Cryptography	The principles, means, and methods for encrypting plaintext and decrypting ciphertext.
Custom Software	Any type of program developed for a particular client or to address a special need.
Customer Engineer (CE)	An individual responsible for field maintenance of computer hardware and software.
Customer-provided Equipment (CPE)	Term applies to equipment owned by the customer or leased from vendors other than the telephone company.
Cybernetics	Cooperative study of the control systems formed by the nervous system and brain in animals and electro-mechanical systems, such as the computer.
Cycle	A repetitive hierarchy. At a systems level, a cycle is often time oriented; e.g., year, quarter, month, or week. Other cycles may represent major repeating sequences in the external world; e.g., fiscal cycle, budget cycle, product cycle.
Data	A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing; any representation, such as characters, to which meaning may be assigned.
Data Access Arrangement	A device that provides direct electrical connection of customerowned and maintained data equipment to the switched telecommunications network.

Data Acquisition	The process of obtaining data from another source, typically one outside the system.
Data, Analog	A physical representation of information such that the representation bears an exact relationship to the original information. The electrical signals on a telephone channel are an analog data representation of the original voice.
Data Analysis (DA)	The function within data management that is used to logically define the enterprise view of objects and design the enterprise logical database model. Data analysis functionally reports to data management and maintains a lateral working relationship with systems analysis, enterprise analysis, data base administration, and data communications administration.
Data Bank	A repository of data; any substantial collection of data.
Database	The aggregate body of all information stored in a computing system that is fundamental to the enterprise which owns or operates the system. Access to the database may be limited to certain specific users and/or application programs.
Data Base Administration (DBA)	The function within data management that is used to design, maintain and implement the enterprise physical data base model and application physical database model.
Data Base Engineering	The discipline of specifying database requirements and designing logical and physical models of the database, both at the application and enterprise levels, which will satisfy the requirements. The objectives of database engineering are: 1) to produce a reliable data base that will satisfy the information needs of the enterprise and perform according to specifications, 2) to produce a data base that is easy to maintain and modify, 3) to physically implement the data base in the most practical, efficient, and cost effective manner possible. Database engineering complements the disciplines of information systems engineering and enterprise engineering.
Database Management System (DBMS)	Computer software used to store and retrieve data based on physical data structure. Normally, the software is limited in use to direct access devices. DBMS packages usually employ either a hierarchical structure, network structure, or relational structure.
Data Classification	To identify and categorize data according to their degree or level of sensitivity and criticality.

Data Collection	The act of bringing data from one or more points to a central point. May be in-plant or out-plant.
Data Communication	The movement of encoded information by an electrical transmission system. The transmission of data from one point to another.
D/D/D	Abbreviation for the design, development, and deployment phase.
Data Dictionary/Directory (DD/D)	A software product that is usually used to control a database management system (DBMS), 4GL or program generator. Unlike an information resource manager, which provides a global and more complete description of all components, the DD/D provides a limited physical description of a component and denotes where it is used in regards to the tool. As such, it is limited to the tool that it is supporting, not to other tools. (See Database Management System).
Data Element	The digital representation of a fact or an event. It is the raw material required to produce information and the basic building block for database modeling. There are three types of data elements: descriptive, indicative, and quantitative. A descriptive data element is used to describe name, routings, addresses, dates, etc. An indicative data element is used to uniquely identify objects and usually consists of identification numbers and codes. Quantitative data elements are those that consist of numeric values, such as quantities and percentages.
Data Element Definition (Yourdon)	A definition that usually includes the data element name, a narrative description, values, and size.
Data Element, Field, Record, File	A single character is called a data element - for example, the number "6". A group of related data elements is called a field or variable, as in the zip code "20548". A group of related fields is called a record, like the name and address of one customer. A group of related records is called a file. A database is a highly organized file or set of files, such as the names and addresses of all customers that comprise a mailing list.
Data encryption standard (DES)	A private key encryption algorithm adopted as the federal standard for the protection of sensitive but unclassified information and used extensively for the protection of commercial data as well.

Data Entry — The process of inputing new data into computer memory, typically from a keyboard.

Data Entry Unit — A unit that transmits data into a computer. For example, a terminal or key-to-disc unit.

Data Flow Diagram (Yourdon) — A diagram that shows each line representing a data element or group of data elements and each circle representing the processing of data.

Data Fusion — The integration of data.

Data Integrity

1. The state that exists when data entered in the AIS are the same as that in source documents, are handled as intended, and are not exposed to accidental or malicious modification, destruction, or disclosure.
2. The preservation of data for their intended use.
3. The property that data have not been altered or destroyed in an unauthorized manner.
4. In a data base system, avoidance of simultaneous update where two concurrently executing transactions, each correct in itself, may interfere with each other so as to produce incorrect results.

See system integrity and software integrity.

Data Management — The orderly and directed control of data from acquisition and input through processing, output, and storage.

Data Manipulation — The processing of information.

Data Medium — The physical material on which data from a computer is stored.

Data Processing (DP) — The execution of a systematic sequence of operations performed upon data. Synonymous with information processing.

Data Rate — The rate at which a communications channel carries data, measured in bits per second (bps).

Data Reduction — The process of transforming raw data into a more compact, more structured, or otherwise more useful form by scaling, smoothing, ordering, or other editing procedures.

Data Set	A device that converts the signals of a business machine to signals that are suitable for transmission over communication lines. It may also perform other related functions.
Data Sharing	The use of a single data file by more than one person or computer. Data sharing can be done by physically transferring files from one computer or individual to another, or it can be done electronically by enabling two or more computers to communicate with each other or with a remote computer on which files are stored.
Data Source	The originator of computer data.
Data Structure	The logical relationships among data units and description of attributes or features of a piece of data (e.g., type, length, etc.)
Data Structure Diagram (Warnier-Orr)	A basic data structure diagram identifies the relationships among data in defining repeating or alternative groups of data.
Data Structured Design	A design process in which the structure of the system process mirrors the structure of the data on which it operates.
Data Transmission	The sending of data from one part of a system to another part. See also Data Communication.
DDP	Distributed Data Processing.
Debug	With software, to detect, locate, and correct logical or syntactical errors in a computer program. With hardware, to detect, locate, and correct a malfunction or to fix an inoperable system. The term *troubleshoot* is more commonly used in hardware contexts.
Decentralized Processing	The distribution of computer-processing facilities and operations in more than one location.
Decision	An internal computer operation or programmed procedure that compares two pieces of information or verifies the status of a single piece of information and then takes a specified action.
Decision/Control System	A system that establishes feedback control for the functional flow.

Decision Support System (DSS)	A set of related programs and the data required to help with analysis and decision making within an organization. A DSS is similar to a management information system (MIS) but provides the user with more help in formulating alternative decisions and choosing the most appropriate course.
Degradation	A condition in which the system continues to operate but at a reduced level of service. Unavailability of major equipment subsystems or components is the usual cause.
Delegation of Procurement Authority (DPA)	Authority to acquire information processing resources up to a specified limit, issued by the General Services Administration in response to an agency procurement request.
Design	A major phase of the systems life cycle. It includes the logical and physical design of the system, producing a detailed systems blueprint.
Design-To-Cost	A method to control cost increases by making achievement of cost goals as important as achieving performance and schedule goals. The principles call for continuous analyses of trade-offs among costs, schedules, and performance requirements and appropriate decisions to keep the program from exceeding preset cost goals.
Desktop Computer	A computer that fits conveniently on the surface of a business desk.
Desktop Publishing	The use of a computer and specialized software to combine text and graphics to create a document that can be printed on either a laser printer or a typesetting machine.
Device	The unit or part of a machine that translates data as input to or output from a computer, i.e., a storage device, a card reader (input), or a printer (output).
Diagnostics	The detection and isolation of a malfunction or mistake in a communications device, network, or system.
Digital Computer	A digital computer is one in which operations are based on two or more discrete states. Binary digital computers are based on two states -- logical on and off -- arrangements of which are used to represent all types of information.
Digital Signature	Encrypted data, appended to or part of a message, that enables a recipient to prove the identity of the sender (and receiver) and resolve any authentication issues between the sender and receiver.

Disaster recovery plan	See Contingency plan, cold site, hot site.
Discretionary access control (DAC)	A means of restricting access to files, directories, or devices. Access controls are discretionary in the sense that a user with a particular access right can pass that access right to any other user. Contrast with mandatory access control.
Disk	A round, flat piece of flexible plastic (floppy disk) or inflexible metal (hard disk) coated with a magnetic material that can be electrically influenced to hold information recorded in digital (binary) form. A disk is, in most computers, the primary means of storing data on a permanent or semipermanent basis.
Disk (Storage)	A method of recording data magnetically on flat rotating disks. The data stored may be accessed randomly rather than sequentially, as on tape storage. Handles huge amounts of storage on-line. Storage is "random access," meaning the recording arms hop around fast to any "address," (location) on any "track" on any disk to "read" or "write" (record) information. Much slower than core, but much less expensive for a given amount of information.
Disk Operating System	Most microcomputers use a disk operating system (DOS), although it may not be called DOS. The DOS is responsible for reading and writing data from and to the disk; it tells the read/write head to move to the appropriate track/sector and reports any errors that may occur during access.
Display	The representation of data in visible form; i.e., cathode ray tube, lights, or indicators on the console of a computer or a printed report.
Distributed Data Processing	Data processing that is performed by connected computer systems at more than one location.
Distributed Database	A database implemented on a network in which the component partitions are distributed over various nodes (stations) of the network.
Distributed Processing	A form of information processing in which work is performed by separating computers that are linked through a communications network.

Documentation	The group of techniques necessary for the orderly presentation, organization, and communication of recorded specialized knowledge in order to maintain a complete record of reasons for changes in variables.
Domain	A specific class of data elements. The domain establishes the set of values that one or more data elements may assume. All data elements have a domain that describes the basic nature of the data element and plays an important role in the establishment of integrity constraints.
DPMA	Data Processing Management Association.
Edit Check	A category of controls built into an AIS to detect unacceptable data values.
Effectiveness	Producing a desired result. Whereas efficiency is concerned with how well a task is performed, effectiveness deals with the necessity of the task itself. Effectiveness answers the question, "Are we doing the right things?"
Efficiency	Producing a desired result without waste. Efficiency is concerned with how well a task is performed. Effectiveness deals with the necessity of the task itself. Efficiency answers the question, "Are we doing things right?"
Electronic Data Interchange (EDI)	The ability to transfer information such as orders and invoices, from one computer to another over a communications network.
Electronic Data Processing (EDP)	This is an all-inclusive term and is liberally interpreted to mean the overall science of converting data by electronic means to any desired form. Synonymous with automatic data processing.
Electronic Funds Transfer Systems (EFTS)	Describes various computerized electronic communications systems that transfer financial information from one point to another. Computer technology is used to expedite the transfer of money without associated paper payment instruments.
Electronic Industries Association (EIA)	Sets industry standards such as interfaces used in data communications.
Electronic Mail	The transmission of messages over a communications network. Electronic mail, or E-Mail, is a computer-to-computer (or terminal-to-terminal) version of interoffice mail or the postal service.

Emulation	A technique to permit a computing system to execute programs written for another system. This form of imitation is primarily done via hardware. Emulation is generally used to minimize the impact of the conversion of programs from one computer system to another.
Encryption	The process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.
End User	Traditionally, the recipient of computer output; with microcomputers, a term used in reference to the people who use (as opposed to design or program) computers and computer applications.
Enterprise Engineering	The discipline of specifying the mission of the enterprise, designing logical and physical models of the enterprise, and developing an enterprise information strategy that is synchronized with business plans. The objectives of enterprise engineering are: (1) To produce a reliable model of the enterprise, (2) To produce a model that is easy to maintain and modify, (3) To develop an information strategy for the enterprise that is practical, efficient, and cost effective.
Enterprise Information Strategy (EIS)	A plan to satisfy the information needs of an enterprise. The plan lists the objectives and projects, in priority ranking, that are required to satisfy the business plan of the enterprise. An EIS is a living document that is constantly evolving and staying in tune with the enterprise.
Enterprise Management	The function concerned with the management of the logical and physical models of the enterprise.
Entity	A thing or class of things that exists independently in the real world.
Entity Diagram	A chart that shows things or classes of things and the transactions that occur between them. It aids the user to put an overall concept of a system down on a single diagram.
Ergonomics	An expression referring to consideration given to the human element in systems design. Systems analysis must consider the human senses and intelligence level as well as man/machine interfaces in determining an appropriate system implementation.

Error	Any discrepancy between a computed, observed, or measured quantity and the true, specialized, or theoretically correct value or condition.
Error Control	An arrangement to detect the presence of errors. In some systems, refinements are added that will correct the detected errors, either by operations on the received data or by retransmission from the source.
Error Correction	System that detects and inherently provides correction for errors occasioned by transmission equipment or facilities.
Error Rate	The ratio of incorrectly received data (bits, elements, characters, or blocks) to the total amount of data transmitted.
Evaluation	A major phase of the systems life cycle. It includes the audit of the system to ensure that it is producing the proper output to solve problems identified in the planning phase.
Execute	To perform a specified operation listed in a program or to run the entire program.
Expert System	A type of application program that makes decisions or solves problems in a particular field, such as finance or medicine, by using knowledge and analytical rules defined by experts in the field.
Feasibility Study	A phase in a project that is used for specifying and analyzing a business problem/opportunity and proposing to management a course of action. It is usually one of the most important phases of a project due to its concentration on the proper identification and specification of business problems and requirements.
Federal Acquisition Regulation (FAR)	The regulation that codifies uniform acquisition policies and procedures for executive agencies governmentwide.
Federal Communications Commission (FCC)	A board of seven commissioners appointed by the President under the Communications Act of 1934, having the power to regulate all interstate and foreign electrical communication systems originating in the United States.
Federal Information Resources Management Regulation (FIRMR)	The regulation that sets forth uniform policies and procedures for acquiring information processing resources, used in conjunction with the FAR.
Fixed-Price Contract	A contract that provides for a firm price, or in appropriate cases, a firm price with fees or other adjustments.

Flexibility	Effort required to modify an operational program.
FORTRAN	FORmula TRANslation Language. A common language primarily used to express computer programs by arithmetic formulas. It is especially adapted to mathematical, scientific, and engineering problems.
Fourth Generation Language	A term applied to languages designed for interacting with the programmer. Such languages are a step up from standard high-level programming languages such as C, Pascal, and COBOL.
Front-End Processor	A dedicated communications computer at the front end of a host computer. It may perform line control, message handling, code conversion, error control, and applications functions such as the control and operation of special-purpose terminals.
Full Scale Development	A phase that includes developing, engineering, fabricating, and testing all items necessary for system support.
Function	A simple mapping of a set of inputs onto an output.
Function Codes	Codes inserted to effect specific machine functions (e.g., tabulate).
Functional Design	The specification of the relationships between working parts of a computer system, including details of logical components and the way they work together.
Functional Flow	A step in the requirements definition phase that includes establishing the main line in terms of information flow using assembly line diagrams.
Functional Requirement	A requirement that specifies a function that a system or system component must be able to perform.
Functional Specification	A description of the scope, objectives, and types of operations to be considered in the development of an information-handling system.
Functional String of Code	A series of software modules that performs a particular function.
Fuzzy Logic	A form of logic used in some expert systems and other artificial intelligence applications in which variables can have degrees of truthfulness or falsehood represented by a range of values between 1 (true) and 0 (false).

Game Theory	A mathematical process of selecting an optimum strategy in the face of an opponent who also has a strategy. The forces of nature might be the "opponent" in a planned space shot. The strategy to overcome these might be "played" on a computer to ascertain an optimum launch date.
General Controls	The controls that apply to overall computer processing carried out at a facility, but these are not related to controls over specific applications.
General-Purpose Computer	A computer that can perform any computational task with software. To change the machine's task, different software is run.
Generation	An informal system of differentiating computer systems as significant technological advances are made. For example, computers using vacuum tubes in one generation, those using transistors in the next and those using integrated circuits in the next.
Graphics	The use of the computer for drawing lines under complete program control, or the attachment of a vector scope and light pen on-line to the computer, enabling the user and the computer to interact and jointly draw pictures on the face of the scope.
Hands-On	An adjective describing practical experience as opposed to theoretical knowledge.
Hardware	The mechanical and electronic equipment combined with software (programs, instructions, etc.) to create an electronic information processing system.
Heuristic Development	Ability to design and refine systems as you go.
Hierarchical Chart (HIPO)	A chart that shows how each function is broken down into subfunctions. For each function or subfunction identified on the hierarchical chart there is an input-process-output chart.
Hierarchical Database	A database in which records are grouped in such a way that their relationships form a branching, treelike structure. Most commonly used with databases for large computers. A hierarchical database is well suited for organizing information that breaks down logically into successively greater levels of detail.

Hierarchical Plus Input-Process-Output (HIPO)	This methodology consists of two components: Hierarchical charts and Input Process-Output charts. The HIPO design process is an interactive top-down activity.
Hierarchical Structure	Refers to how data is structured in a file. In this structure, a file is organized into a hierarchy of records with superior/subordinate relationships. Each level has only one "parent" but can have multiple "children."
Hierarchy	The relationship between a set, its subsets, and its elements. A structured hierarchy requires that the relationship between the elements of any level must be sequence, alternation, repetition, recursion, or concurrency.
High-Level Language	Since writing languages in a low-level language can be tedious and complicated, languages were further developed to use English-like statements and symbols rather than assembly language mnemonics. A high-level language is also very compact, almost like a form of short-hand. One high-level language statement can be the equivalent of many machine instructions, where as a low-level language requires one statement for each machine instruction.
Host Computer	The primary or controlling computer in a multiple computer network operation. This computer normally provides high-level services, such as computation, data base access, or special programs or programming languages for other computers in the network. A computer used to prepare programs for use on another computer or on another data processing system; for example a computer used to compile, link, edit, or test programs to be used on another system.
Hot Site	A fully equipped computer center that provides an alternative computing capability for use in the event of a disaster, such as flood or fire. Contrast with cold site.
Housekeeping	Operations or routines that do not contribute directly to the solution of the problem but do contribute directly to the operation of the computer.
Human Engineering	The designing of machines and associated products to suit the needs of humans.
Human Safety	Freedom from those conditions that can cause death or injury, or damage to or loss of data, hardware, or software.

Human-Machine Interface	The boundary at which people make contact with and use machines, more typically known as the user interface when applied to programs and operating systems.
I/O	Input/output.
Identification	The process of telling a system the identity of a user or another system. Usually part of the login process. See also authentication.
Implementation	A major phase of the systems life cycle. It involves putting a constructed system into effect in a particular physical environment.
Information Management System (IMS)	A program product that uses IBM's Operating System and BTAM to allow special applications to operate on the remote terminal system.
In-Out Diagram	Used to document data flow from an operational standpoint.
Increment	To increase the value of a number, usually by one.
Independent Verification and Validation (IV&V)	Verification and validation performed by an organization that is technically, managerially, and financially independent of the development organization.
Information	1. The meaning that is currently assigned to data by means of the conventions applied to that data. 2. In a conceptual schema language, any kind of knowledge about things, facts, or concepts of a universe of discourse that is exchangeable among users.
Information Costs	The costs incurred in acquiring and/or producing information. This includes the cost of the resources used to produce information and other related expenses incurred in its production, storage, and dissemination. This production of information, from an accounting standpoint, is similar to the production (manufacture) of a commodity. Both involve converting something raw (unfinished) to a finished product by applying resources such as direct labor (people), equipment, and overhead.
Information Engineering	An integrated set of formal techniques for planning, analysis, design, and construction of information systems from a enterprise-wide perspective.

Information Flow	The sequence, timing, and direction of how information proceeds through an organization.
Information Life Cycle	Describes the stages of information processing beginning with creation or collection and proceeding through final disposition.
Information Management	The overall management and control of information, including identifying and sharing of management information needs; ensuring standardization, control, security, and integrity of data stored or manipulated; statistical records and management activities; and the privacy of records and freedom of information considerations.
Information Processing	The acquisition, storage, manipulation, and display of data, particularly by electronic means.
Information Requirement	A user need for specific information in order to perform duties and responsibilities.
Information Resources Management (IRM)	The planning, budgeting, organizing, directing, training, promoting, controlling, and other management activities associated with burden collection, creation use, and dissemination of information by an agency and including the management of information and related resources such as automatic data processing equipment. The process of (1) defining in a systematic way the information needed to effectively accomplish an agency's missions, goals, and objectives and (2) managing information resources to efficiently and economically meet the defined information needs.
Information Retrieval	The process of finding, organizing, and displaying information particularly by electronic means.
Information Science	The study of how information is collected, organized, handled, and communicated.
Information Security	Generally considered to be the overall management, procedures, and controls necessary to ensure confidentiality, integrity, and continuity of operations for an information system.
Information Systems	A support mechanism for the information life cycle that assists in the production, administration, processing, protection, and storage of the information asset.

Information Systems Engineering	The discipline of specifying user information requirements, designing a logical system that can produce the required information, determining the most appropriate way to physically process data, and to successfully implement the physical system. The objectives of information systems engineering are: (1) to produce a reliable information system that will satisfy user information requirements and perform according to specifications and (2) to produce an information system that is easy to maintain and modify.
Information Technology (IT)	The computing and telecommunications hardware and software that carry and process data, sound, and video in support of the information life cycle.
Initiation, Project	The process of initiating a project when a work request has been approved.
Input	Material entered into a data or word processing system for processing. Also, the transfer of data to be processed from keyboard or an external storage device to an internal storage device.
Input/Output Device	A piece of hardware that is used for both providing information to the computer and receiving information from it.
Input-Output (I/O)	A general term for the equipment used to communicate with a computer and the data involved in the communications.
Input-Process-Output Chart (HIPO)	A chart that shows the inputs and outputs to each function and the processes each function performs with those inputs and outputs.
Integrated Software	A category of application program that continues several computer tasks, such as word processing, database management, and spreadsheets, in a single package.
Integration	The sharing of data or information among subsystems and systems.
Integrity	The completeness and accuracy of data stored in a computer, particularly after it has been manipulated in some way.
Intelligent Terminal	A terminal with its own memory, processor, and firmware that can perform certain functions independent of its host processor.

Interactive	Operating in a back-and-forth, often conversational manner, as when a user enters a question or command and the system immediately responds.
Interconnectivity	The ability to link equipment electronically, e.g., to attach to a network and send and receive data.
Interface	The point at which a connection is made between two elements so that they can work with one another. In computing, different types of interfacing occur on different levels, ranging from highly visible user interfaces that enable people to communicate with programs to often invisible, yet necessary, hardware interfaces that connect devices and components inside the computer.
Intermittent Error	An error that recurs at unpredictable times.
Internal Control	The plan of organization and methods and procedures adopted by management to ensure that resource use is consistent with laws, regulations, and policies; that resources are safeguarded against waste, loss, and misuse; and that reliable data are obtained, maintained, and fairly disclosed in reports.
Interoperability	The ability of systems to work together, to send and interpret messages, share data, etc.
Interoperability	The ability of information technology resources to provide services to and accept services from other resources.
Interoperate	To provide services to or accept services from other systems, subsystems, or components and to use the exchanged services effectively.
Invitation for Bid (IFB)	The solicitation document used when contracting by sealed bidding.
Knowledge Base	A form of database used in expert systems that contains the accumulated body of knowledge of human specialists in a particular field.
Language	A system for representing and communicating information or data between people, or between people and machines. Such a system consists of a carefully defined set of characters and rules for combining them into larger units, such as words or expressions, and rules for word arrangement or usage to achieve specific meanings.

Large Scale Computer	Large-scale computers provide complex and powerful programmable logic to attack complex problems which require highly centralized computing power. Examples include, CDC 7600, CRAY, AMDAHL 470, ILLIAC IV, and others. Some operate at speeds of 100 million instructions per second.
Life Cycle	See systems life cycle.
Life Cycle Costs	The cost to design, develop, deploy, operate, and maintain a system throughout its designated life.
Line	A line of information in a computer program.
Line of Code	A single computer program command, declaration, or instruction. Program size is often measured in lines of code.
Liquidated Damages	Compensation to the government for a contractor's failure to perform in a timely manner.
Listing	A report printout.
Local Area Network	A communication system designed for intra-building data communications.
Local Area Network (LAN)	A group of computer and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.
Logic	The systematic scheme, which defines the interactions of signals in the design of a program, system, etc.
Logic Chart (Chapin Chart)	First used as a modeling tool to aid in the development of structured programs.
Logic Diagram	A schematic that shows the connections between computer logic circuits specifying the expected outputs from a specific set of inputs.
Logical Bases Files (LBF)	Logical files of entities, relationships, or cycles shown with their appropriate data elements. The minimal data requirements.
Logical Data Structure (LDS)	A logical data hierarchy derived from the logical output structure (LOS) of an output, less any computed, redundant, and literal data elements, sometimes with structural information added.

Logical Decision	Any decision that can have one of two outcomes (true/false, yes/no, and so on).
Logical Output Structure (LOS)	All the data elements for a particular output shown mapped onto its hierarchical structure.
Logical Process Structure (LPS)	The logical hierarchy of a process.
Logical Set	A set of actions or data processed the same number of times and under the same conditions or at the same place.
Logical System Definition	The planning of an automated information system prior to its detailed engineering design. This would include the synthesis of a network of logical elements that perform specific functions.
Logical Tools	Tools that are independent of computers and computer languages.
Low-Level Language	A language that is machine-dependent and/or that offers few control instructions and data types. Each statement in a program written in a low-level language usually corresponds to one machine instruction. Assembly language is considered a low-level language.
LSI	Large scale integration.
MAC	Abbreviation for 1. message authentication code and 2. mandatory access control.
Machine	A general name for equipment that can store and process numeric and alphabetic information.
Machine Independent	A program or piece of hardware that can be used on more than one computer with little or no modification.
Machine Language	The internal binary language into which more advanced programming languages must be converted before a computer can process a computer program.
Machine Readable	Information presented in a form that a computer can interpret and use as input.

Machine-Dependent An adjective describing a program or piece of hardware that is linked to a particular computer because it makes use of specific or unique features of the equipment that cannot easily, if at all, be used with another computer.

Macro In applications, the program carries out the instructions of the macro. Program users create macros to save time. Macro instructions can be placed either in the program itself or in a separate file on the floor that is identified in the program. Macros are replaced by the actual instructions they represent when the program is prepared for execution.

Mainframe Mainframe computer.

1. The central processor of the computer system. It contains the main storage, arithmetic unit, and special register groups. Sometimes called central processing unit (CPU).

2. All that portion of a computer exclusive of the input, output, peripheral, and, in some instances, storage units.

Mainframe Computer A high-level computer designed for the most intensive computational tasks. Mainframe computers are often shared by multiple users connected to the computer via terminals.

Maintainability The ease with which maintenance of a functional unit can be performed in accordance with prescribed requirements.

Maintenance The periodic modification of information, i.e., files, programs, etc., to incorporate changes that occurred during a given period or that have been requested by outside sources.

Management Information System A computer-based system of processing and organizing information so as to provide different levels of management within an organization with accurate and timely information needed for supervising activities, tracking progress, making decisions, and isolating and solving problems.

Mandatory Access Control A means of restricting access to files, directories, or devices. Mandatory access controls use sensitive system. Those access rights cannot be passed on to another user. Contrast with discretionary access control.

Mapping	The process of changing some given input into a given output through a rule of transformation. There are four types of mappings: one to one; one to many; many to one; and many to many.
Market Survey	Attempts to ascertain whether other qualified sources capable of satisfying the government's requirement exist. This testing of the marketplace may range from written or telephone contacts with knowledgeable federal and non-federal experts regarding similar or duplicate requirements and the results of any market test recently undertaken, to the more formal sources-sought announcements in pertinent publications (e.g., technical/scientific journals, the *Commerce Business Daily*), or solicitations for information or planning purposes.
Master File	A main reference file of information used in a computer system. It provides information to be used by the program and can be updated and maintained to reflect the results of the processing operation.
Matrix	An array of quantities in a prescribed form.
Media	A collective word for the physical material, such as paper, disk, and tape used for storing computer-based information.
Medium	The material on which data are recorded (paper tape, punch cards, magnetic tape, etc.).
Microcomputer	A complete tiny computing system consisting of hardware and software whose main processing blocks are made of semiconductor integrated circuits. In function and structure, it is somewhat similar to a minicomputer with the main difference being price, size, speed of execution, and computing power.
Microprocessor	A small integrated circuit that contains the complete central processing unit for a small digital computer. A microcomputer is made by connecting a memory integrated circuit to a microprocessor.
Minicomputer	A small programmable general-purpose computer typically used for dedicated applications. Minicomputer often refers only to the central processing unit. Usually, it is a parallel binary system with 8-, 12-, 16-, 24-, or 36-bit word length incorporating semiconductor or magnetic core memory.
MIPS	Acronym for millions of instructions per second, a common measure of processor speed.

Management Information System (MIS)	Management Information System. A data processing system that is designed to furnish management and supervisory personnel with current information to aid in the performance of management functions. Data is recorded and processed for operational purposes, problems are isolated and referred to upper management for decision-making, and information is fed back to reflect progress in achieving major objectives.
Mode	A method of operation (as in binary mode, alphameric mode, etc.).
Model	An abstraction from a real situation that makes predictions in the real world possible.
Modem	MOdulator-DEModulator. A device used in a communications system to convert digital data processing signals into analog or voice-like signals for transmission over a telephone line. At the other end of the line, another modem converts the analog signals back into digital form.
Modem (Data Set)	Contraction of modulator-demodulator. A device to convert one form of signal to another form for compatibility.
Modification/ Improvement (MOD/IMP)	The activity required to change or enhance an existing product. For most IRM organizations, this will represent 85 percent to 90 percent of their work effort.
Modular Program	A program that can be characterized as 1. implementing a single independent function, 2. performing a single logical task, 3. having a single entry and exit point, and 4. being separately testable.
Modular Software	Software that is in self-contained, logical sections or modules, which carry out well-defined processing actions.
Module	An interchangeable plug-in unit or a compatible add-on unit.

MS-DOS, CP/M, UNIX, Apple DOS	One popular operating system for small computers is MS-DOS MicroSoft Disk Operating System, of which there are several versions. Other examples of popular operating systems are CP/M, UNIX, and Apple DOS. A program written on one computer can be used or easily adapted on another, provided that both use the same version of the same operating system and the same disk formats.
Multilevel security	A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present.
Multiprocessing	Using several computers hooked together to accomplish running of programs, data, or information.
Multiprocessor	A computer with multiple arithmetic and logic units for simultaneous use.
Multiprogramming	A technique for handling numerous routines or programs simultaneously by means of an interweaving process.
Multitasking	A mode of operation offered by an operating system in which a computer works on more than one task at a time.
National Information Infrastructure (NII)	NII is the initiative supporting the fiberoptic information superhighway. The superhighway is expected to be the foundation for the national information network, envisioned to reach into every home, school, library, government agency, and business.
Need-to-know	A determination that a prospective recipient of sensitive information has a legitimate requirement to access, to have knowledge of, or to possess that information.
Network	A series of points interconnected by communication channels. The switched telephone network consists of public telephone lines normally used for dialed telephone calls. A private network is a configuration of communication channels reserved for the use of a sole customer.
Network Architecture	The underlying structure of a computer network, including hardware, functional layers, interfaces, and protocols (rules) used to establish communication and ensure the reliable transfer of information.

Network security	Techniques and practices that 1. limit remote access to AIS resources, and 2. protect transmitted information from unauthorized surveillance and alteration.
Networking	Hooking geographically separated computers together over transmission lines. This allows computers to ship data to each other or ship jobs around (either in case of overload or because one of the many computers has the necessary computer programs or data to do a particular job). In teleprocessing, a number of communication lines connecting a computer with remote terminals. In general communication applications, the interconnection of multiple communication channels, multiple terminals, and/or computers (nodes).
Neural Network	A type of artificial-intelligence system modeled after the neurons (nerve cells) in a biological nervous system and intended to simulate the way in which a brain processes information, learns, and remembers.
Node	Any station, terminal installation, communications computer, or communications computer installation of a computer network.
Node	A system (or workstation) connected to a network.
Object Program	A machine language program ready for execution, usually the output of a coding system. Contrasted with source program.
Off-the-Shelf	Ready-to-use, packaged. The term can refer to hardware or software.
Office Automation	The use of electronic and communications devices such as computers, modems, and fax machines as well as any associated software to perform office functions mechanically rather than manually.
On-Line System	A system in which the data to be input enter the computer directly from the point of origin (which may be remote from the central site) and/or the output data is transmitted directly to the location where it is to be used.

Open Architecture	A term used to describe any computer or peripheral design that has published specifications.
Open Shop	The operation of a computer facility where computer programming, coding, and operating can be performed by any qualified employee of the organization, not necessarily by the personnel of the computing center itself, and where the programmer may assist in or oversee the running of his program on the computer. Contrasted with closed shop.
Open System	In communications, a computer network designed to incorporate all devices--regardless of manufacturer or model--that can use the same communications facilities and protocols.
Operating System (OS)	An integrated collection of service routines for supervising the sequencing of programs by a computer. Operating systems may perform debugging, input-output, accounting, compilation, and storage assignment tasks.
Operation (Computer)	The electronic action resulting from an instruction. In general, it is a computer manipulation required to secure results.
Operational Information	The type of information required to conduct the fundamental business of the enterprise.
Optimization	In programming, the process of producing more efficient (smaller and/or faster) programs through the selection and design of data structures, algorithms, and instruction sequences.
Orange Book	Synonym for Trusted Computing System Evaluation Criteria.

Organizing	Organizing to incorporate the institutional objectives determined in planning means establishing the most efficient, effective, and economical relationships between functions and people. Organizations and related structures should be subject to continuing reviews of missions, goals and objectives and the effects of changes in circumstances (e.g., technological tools for carrying on business activity). Organizing and organizational structures should clearly convey major missions and objectives, activities, and primary functions and duties; delineation of authorities, roles, positions, and accountabilities and responsibilities for achieving them; and the structure of organizational activities necessary to best attain objectives and provide responsible managers with appropriate authority and effective lines of communication.
Original Equipment Manufacturer (OEM)	The OEM makes a product for assembly into a final system or larger subassembly by another manufacturer. Frequently, OEM's make computer peripherals that are integrated into a complete system by a mainframe vendor.
OS/VS	Operating System/Virtual Storage.
Output	Information transferred from the computer to the outside world. As an adjective, pertaining to the devices which bring information out of the computer.
Output Oriented Design	Design that starts with the output and works backward.
Packaged Software	A software program sold through a retail distributor as opposed to custom software.
Packaging	The process of grouping logical data and action structures into machine or human processable units.
Parallel Processing	A method of processing that can run only on a type of computer containing two or more processors running simultaneously.
Parallel Run	Running of a newly developed system in a data processing area in conjunction with the continued operation of the current system.

Path	A route from one point to another. In communications, a path is a link between two nodes in a network. In a database, a path is the selection of branches and nodes to be traversed in a tree structure in order to progress from the root node of the tree to any other node. In programming, a path is the sequence of instructions a computer carries out in executing a routine. In file storage, a path is the route followed by the operating system in finding, storing, and retrieving files on a disk.
Payout	Payout (or Payoff) Period. The time it takes for an investment (e.g., in a new machine) to pay for itself.
Peer Review	A quality assurance method in which peers review a programmer's work for accuracy and for consistency with the other parts of the system.
Performance Management	The process of analyzing the performance of a computer system to determine how resources are currently utilized and how such utilization can be improved. Capacity planning assists in forecasting computer resource requirements to ensure that capacity exists when needed.
Performance Validation	The technical verification of the ability of a proposed system configuration or replacement component to handle agency-specific workload volumes (present and expected) within agency-determined performance time constraints.
Phase	A prescribed set of one or more activities normally performed serially to accomplish specific work. One or more phases make up a project. The sequence by which they are executed indicates the project structure (methodology) and is usually based on the structure of the product to be produced. Phases also usually have deliverables associated with them.
Physical Design	Adding physical constraints, restrictions, and volumes to a logical systems design.
Physical Security	Security measures taken to protect automated information systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion, deliberate attacks, and accidents. Physical security is achieved through the use of locks, guards, badges, fences, and administrative controls. (FIPS 41 Sec. 1.3 and 3)

Project Plan	A formal plan for executing a project. A project plan specifies (1) what project will be executed and when, (2) what resources will be required, (3) what methodology will be followed, (4) what work requests will be implemented by the project, (5) what user organizations will be directly affected by the project, (6) what other organizations will be directly affected by the project, and (7) what other pertinent components will be affected; i.e., systems, outputs, inputs, files, etc.
Planning	A major phase of the systems life cycle. The identification of problems to be solved by a system.
Platform	The foundation technology of a computer system.
Precision	The extent of detail used in expressing a number. Precision indicates degree of detail; accuracy indicates correctness.
Preventive Maintenance (PM)	Upkeep operations necessary to keep equipment running in good order, including regular cleaning, replenishment of expendable supplies, and the replacement of worn or expendable parts. Some of these functions are usually handled by manufacturer service representatives in accordance with a general equipment maintenance contract.
Privacy	Legislation that requires agencies to restrict the collection and use of personal information about individual U.S. citizens to official uses only and requires safeguards to protect the integrity of the information.
Procedure	A logical description of a set of actions to accomplish a task. A procedure may be implemented using either manual or computer means.
Process Description (Yourdon)	A structured English narrative explaining how the data is manipulated in each bubble in structured design methodology.
Processing	Manipulating data within a computer system.
Processing Method	An expression used to describe the approach taken for the execution of information systems including such methods as interactive, on-line, real-time, transaction, batch, data and time driven. The method selected depends upon the derived logical processes and is based upon the analysis of timing and economics required to meet the information needs.

Processor	A computer capable of receiving data, manipulating it, and supplying results.
Procurement	The actual process of acquiring the product or services.
Productivity	Producing results. It is measured by effectiveness ("Are we doing the right things?") and efficiency ("Are we doing things right?"). productivity = effectiveness + efficiency.
Proficiency	Refers to the level of knowledge or skill of a particular worker. It is used to measure a worker's overall proficiency, a resource's current job proficiency, and the specific skills of a resource.
Program	The set of instructions a computer follows to process and deliver its answer or information requested.
Program Analysis	The function in systems management that is concerned with developing computer procedures and programs based on subsystem specifications. Program analysts should have detailed technical knowledge of both computer hardware and software. Skilled programmers should be able to adapt readily to various machines and programming languages because of their in-depth understanding of computer technology and principles.
Program Design Methodology	Structured design methods including: 1. functional decomposition, 2. data flow design, 3. data structure design, and 4. programming calculus.
Program Diagram (Warnier-Orr)	A program diagram provides a method of defining the logic of a process.
Program Maintenance	The process of supporting, debugging, and upgrading a program in response to feedback from individual or corporate users or the marketplace in general.
Program Manager	The key management official who represents the program office in formulating resource requirements and managing presolicitation activities. In some organizations, the program manager or another management official is designated as the acquisition manager for a specific acquisition.

Programming	Designing, writing, and testing computer programs. Depending upon the philosophy of the particular institution, programming can include substantial amounts of systems analysis.
Programming Language	Any artificial language that can be used to define a sequence of instructions that can ultimately be processed and executed by the computer.
Project	A scope of work consisting of one or more phases. A project is an application of the material and human resources to a specific objective through the execution of a prescribed sequence of events. All projects have a structure that usually consists of a beginning, a middle, and an end.
Project Evaluation	Usually the last phase of a project which is used to evaluate estimated versus actual costs and dates for both development and operation.
Project Life Cycle	An expression that is commonly used to refer to the life of a project, from its inception to its conclusion.
Project Management	The function of applying resources to a defined goal and obtaining this goal within time and cost objectives. There are six basic activities involved with project management: project initiation, planning, estimating, scheduling, reporting, and control. A project manager should have leadership skills and an appreciation of planning and control. This function is sometimes called project leader, team leader, foreman, or contractor.
Proprietary Software	A program owned or copyrighted by an individual or a business and available for use only through purchase or by permission of the owner.
Protest	A written objection by an interested party to (1) a solicitation for a proposed contract, (2) a proposed award, or (3) the award of a contract.
Prototype	A process by which a system can be built by a "quick and dirty" method in response to users' needs. The systems are then refined and modified as they are used, in a continuous process, until the fit between user and system is acceptable
Public-Domain Software	A program donated for public use by its owner or developer and freely available for copying and distribution.

Quality Assurance (QA)	A function that is concerned with building quality into a product during design, rather than inspecting for quality after the fact. Quality assurance is a shared responsibility and not a single job description in a company. Quality is judged by how well the product conforms to specifications. An effective QA program for IRM includes an IRM engineer, project administrator and technical librarian.
Queued Telecommunications Access Method (QTAM)	A software protocol that provides the capabilities of BTAM, plus the ability to queue messages on direct-access storage devices. QTAM is employed in data collection, message switching, and many other teleprocessing applications.
Queuing Theory	A form of probability theory useful in studying delays or line-ups at servicing points.
Range	In general usage, range refers to the spread between specified low and high values. Range checking is an important method of validating data entered into an application.
Rapid Prototyping	A type of prototyping in which emphasis is placed on developing prototypes early in the development process to permit early feedback and analysis in support of the development process.
Raw Data	Data that has not been processed. Such data may or may not be in machine-sensible form.
Real Time	The processing of transactions as they occur rather than batching them. Pertaining to an application in which response to input is fast enough to affect subsequent inputs and/or guide the process control system or a computer-assisted instruction system.
Real Time Processing	Operations performed on a computer simultaneously with a physical process or activity such that the answers obtained through the computer operations can affect the process or activity.
Realization	A particular physical implementation of a logical design.
Record	A group of related facts or fields of information treated as a unit.
Record Layout	The organization of data fields within a record.
Recovery	The actions necessary to restore a system and its data files after a system failure or intrusion.

Recursion	The repetition of a logical hierarchy. In general, a process or data that uses itself as a part of its definition.
Redundancy	That portion of the total information contained in a message that can be eliminated without the loss of essential information, such as characters used only for checking. Also used to describe a computer or communications facility in which there is a spare backup device for each important component of the system.
Relational Database	A type of database or database management system that stores information in tables--rows and columns of data--and conducts searches by using data in specified columns of one table to find additional data in another table.
Relational Structure	Refers to how data is structured in a file. In this structure a file or table is not organized by owners and pointers as in the hierarchical and network structures, but rather data is organized into records or columns with primary and foreign keys that are used to make up relationships between data.
Relationship	An intermediate set that resolves a many-to-many mapping, such as invoice, transaction, etc.
Reliability	The extent to which a system or program can be expected to perform its intended function with required precision.
Remote	Not in the immediate vicinity. An adjective used to describe a computer or other device located in another place that is accessible through some type of cable or communications link.
Remote Access	An arrangement whereby distant workstations have access to a central computer via communications channels.
Request for Comment	An announcement in the *Commerce Business Daily* or other publication requesting industry comment on draft specifications for resources.
Request for Proposals (RFP)	The solicitation document used in negotiated procurements to communicate government requirements and to solicit proposals.
Requirements Definition	A major phase of the systems development life cycle. It involves the identification of system outputs and information and the functional analysis of the requirements for the proposed system.

Resource	A reusable source of supply to produce something. Examples include human, financial, material, and information resources. To maximize the efficient and effective use of resources, they must be classified in order to share them and eliminate unwanted redundancy and controlled in order to receive, store and distribute them properly.
Response Time	The time a system takes to react to a given act: the interval between completion of an input message and receipt of an output response. In data communications, response time includes transmission time to the computer, processing time at the computer (including access of file records), and transmission time back to the terminal.
Responsibility	Specific duties that must be performed to fulfill a function. A function is a grouping of responsibilities.
Return on Investment	The ratio of projected cost savings versus amount invested.
Ring Network	A local area network in which devices (nodes) are connected in a closed loop, or ring. Messages in a ring network pass in one direction, from node to node. Each node examines the destination address attached to the message; otherwise, the node regenerates the signal and passes the message along to the next node in the circle.
Risk	The potential effect if a threat exploits a particular vulnerability of a system.
Risk Analysis	An analysis of system assets, threats, and vulnerabilities to establish an annual loss expectancy (ALE) or equivalent for certain events based on costs, potential losses, harm or damage, and estimated probabilities of the occurrence.
Risk Assessment	A process performed during the initiation of AIS development that provides an estimate of the damage, loss, or harm that could result from a major failure. Contrasts with a risk analysis in that a risk assessment does not identify controls and safeguards.
Risk Management	A management approach to balancing the costs and benefits of AIS security to ensure that AIS's are protected by a cost-effective mix of security safeguards and controls commensurate with the risks to the AIS and the mission it supports.
RPQ	Request for price quotation.

Safeguards	Synonym for security controls.
Schema	A schema defines a particular view of some aspect of the database; that is, it defines the attributes (or fields) that will be visible, the domains (permissible values) of the attributes, and information concerning the form and location of attributes. A description of a database to the database management system (DBMS), generated using the data definition language provided by the DBMS.
Security	Preservation of the authenticity, integrity, confidentiality, and ensured service of any sensitive or nonsensitive system-valued function and/or information element.
Security Controls	Any action, device, procedure, technique or other measure that achieves effective computer and information security. Security controls are a subset of internal controls.
Security Goals (Objectives)	The three goals of AIS security are to achieve an acceptable degree of 1. data and software integrity (accuracy); 2. data confidentiality; and 3. system and data availability.
Security Management	Management activities including planning, budgeting, organizing, training, controlling, and project management that are implemented to ensure cost effective AIS security.
Security Plan	See system security plan.
Security Policy	The laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Security Testing	A process used to determine that the security features of a system are implemented as designed and are effective in operation.
Sensitive Information	Any information for which the loss, misuse or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of federal programs or the privacy to which individuals are entitled under the Privacy Act, but which is not considered as classified information.

Shared Logic System	Multi-terminal (operator console) systems where each terminal shares the word processing power, storage, and peripherals of a central computer. Included in this category are distributed logic systems that share peripherals and sometimes storage, but have most computer power distributed at the individual operator stations.
Shared Resource	Any device, data, or program that is used by more than one other device or program.
Simulation	1. The representation of physical systems and phenomena by computers, models, or other equipment; e.g., an imitative type of data processing in which an automatic computer is used as a model of some entity or process. Information enters the computer to represent the factors entering the real process, the computer produces information that represents the results of the process, and the processing done by the computer represents the process itself. 2. In computer programming, the technique of setting up a routine for one computer to make it operate as nearly as possible like some other computer.
Simultaneous Processing	The term is generally used to refer to concurrent operations in which more than one task is processed by dividing processor time among the tasks.
Skill	A developed aptitude or ability for performing a specific activity or activities within a particular enterprise.
Skills Inventory	An accounting of the skills possessed by human resources. Proficiency ratings are also noted.
Software	The totality of programs and routines used to extend the capabilities of computers, such as compilers, assemblers, narrators, routines, and sub-routines. Contrasted with hardware.

Software Engineering	A subset of information systems engineering that is concerned with the analysis of computer processing specifications, designing programs that will be the most appropriate solution to satisfying these specifications, defining the machine operating instructions for executing the programs, and successfully producing executable object code for a computer. The objectives of software engineering are (1) to produce reliable programs that will perform according to specifications, (2) to produce programs that are easy to maintain and modify, (3) to physically implement programs in the most practical, efficient, and cost effective manner possible.
Software House	Refers to a company that offers software support service to users. This support can range from simply supplying manuals and other information to a complete counseling and computer part-time programming service (job shop or body shop).
Software Package	Data, programs, and assistance provided by a vendor and usually at least partially modified for the user's computer systems configuration.
Software Tools	Programs, utilities, libraries, and other aids that can be used to develop programs more efficiently.
Solicitation	An official government request for bids/proposals generally publicized in the *Commerce Business Daily* in accordance with federal regulations.
Source Data	The original data on which a computer application is based; for example, employee job applications and performance reports might be the source data for a company's employee database.
Source Document	An original record of some type that is to be converted into machine readable form.
Source Selection Authority (SSA)	The government official in charge of selecting the source for an acquisition. Most often the title is used when the selection process is formal and the official is other than the contracting officer.
Source Selection Evaluation Board (SSEB)	A board composed of technical, contract, information resources managers, and other government personnel whose primary function is to evaluate proposals received in response to a request for proposal.

Source Selection Plan	A document that describes the entire process for awarding a contract--proposal evaluation criteria, evaluation methodology, evaluator's responsibilities, and final selection procedures.
Spatially Referenced Information	Information that can be associated with a specific place on the earth's surface, such as the exact geographic location of a lake, road, or stand of trees.
Specific Make and Model Specification	A description of the government's requirement for resources that is so restrictive that only a particular manufacturer's products will satisfy the government's needs.
Specification	A detailed description. In relation to computer hardware, specifications provide information about the machine's components, capabilities, and special features. In reference to software, specifications describe the operating environment and proposed features of the new program. In information processing, specifications describe data records, programs, and procedures involved in a particular task.
Stand-Alone	An adjective describing a device or an operation that does not require support from another device or system.
Standalone System	A system that does not share the processing power of a central computer.
Standard	In computing, a set of detailed technical guidelines used as a means of establishing uniformity in an area of hardware or software development.
Star Network	A computer network with peripheral nodes all connected to one or more computers at a centrally located facility.
Statement of Work (SOW)	A technical description of resources, prepared for inclusion in a solicitation document.
Steering Committee	The steering committee can provide valuable assistance to the information resource management function for setting direction and relieving any pressures between the project team and the user. It should be composed of members from enterprise management, user management, and information resource management. It also establishes project priorities in line with company policy and objectives.

Strategic Plan	A set of objectives dealing with the future direction of the enterprise, either for survival or competitive advantage. This includes developing new products or services, expanding existing offerings, entering new markets, diversifications, acquisitions, mergers, etc.
Structural Analysis	A method of analysis that addresses: 1. code-level, 2. module level, 3. software system level.
Structure	The arrangement or interrelation of parts as dominated by the general character of the whole.
Structured Design	A method of design that employs only the structured constructs: sequence, repetition, alternation, hierarchy, concurrency, and recursion.
Structured Programming	A general term referring to programming that produces programs with clean flow, clear design, and a degree of modularity or hierarchical structure.
Subsystem	A secondary or subordinate system usually capable of operating independently of, or asynchronously with, a controlling system.
Suite	A group of related programs.
Supercomputer	A large, extremely fast, and expensive computer used for complex or sophisticated calculations.
Support	Assistance -- for example, the technical advice provided to customers by the manufacturer or developer of a hardware or software product. To work with another program or product.
System	A set of interrelated processes or elements that collectively work together to achieve some common purpose or goal.
System Administrator	The person responsible for administering the use of a multiuser computer system, communications system, or both.
System Analysis	The examination of an activity, procedure, method, technique, or a business to determine what must be accomplished and how the necessary operations may best be accomplished.

System Decision Papers	The primary documentation used for obtaining approval of major decisions at milestone points during system development.
System Development	The process of defining designing, developing, testing, and implementing a new system.
System Development Life Cycle	The portion of the system life cycle that involves development activities.
System Development Life Cycle Methodology	The process of dividing the automated system development process into distinct phases and providing for periodic management review. Federal Information Processing Standards Publications 38 and 64 divide the process into three phases: initiation, development, and operation.
System Life	A projection of the time period that begins with the installation of the resource and ends when the agency's need for that resource has terminated.
System Life Cycle	The three identifiable phases of an AIS including initiation, development, and operation. See systems development life cycle.
System Parameter	A factor or property whose value determines a characteristic or behavior of the system.
System Security Plan	A basic overview of the security and privacy requirements of an automated information system and the agency's plan for meeting those requirements.
System Software	The collection of programs and data that make up and relate to the operating system.
Systems Engineering	The systematic application of technical and managerial processes and concepts to transform an operational need into an efficient, cost-effective system using an iterative approach to define, analyze, design, build, test, and evaluate the system.
Systems Integration	The development of a computer system for a particular customer by combining products from different original equipment manufacturers.
Systems Integrator	The process by which a contractor that teams with different vendors to create a system and usually does not manufacture its own equipment. Prime contractors can, however, serve as integrators without teaming. An agency can also serve as the integrator, as can a manufacturer.

Systems Management	A function that is responsible for the development, modification/improvement, and maintenance of information systems within an enterprise. As such, it is a management function, not an administrative function. It is concerned with developing information systems that satisfy the requirements of the enterprise.
Systems Network Architecture (SNA)	Refers to IBM's standardized relationship between its virtual telecommunication access method (VTAM) and the network control program (NCP/VS).
Systems Objectives	Measurable goals of a system.
Systems Programming	The development or maintenance of programs designed to execute as part of an operating system.
Tactical Plan	A set of objectives dealing with how to improve the internal operations of an enterprise. They are aimed at maximizing productivity and minimizing costs. This includes work simplification/efficiency, resource management, production control, etc.
Technical Integrity	The characteristic of producing proper output response for a given input stimulus.
Technical Leveling	Helping an offeror to bring its proposal up to the level of other proposals through successive rounds of discussion, such as by pointing out weaknesses resulting from the offeror's lack of diligence, competence, or inventiveness in preparing the proposal.
Technical Library	The central repository for all project/systems documentation and records. The contents of the technical library represent a considerable investment by the company. In addition, the library contains company know-how. For these reasons alone, the maintenance and operation of a library with tight control is justified. Without control, project documentation can become misplaced and out of date very quickly. It is for these reasons that the technical librarian works closely with the project administrator.
Technique	A synonym for procedure or process.
Technology	The application of science and engineering to the development of machines and procedures in order to enhance or improve human conditions, or at least to improve human conditions or human efficiency in some respect.

Telecommunications	The reception and/or transmission of information of any nature by telephone, telegraph, radio, or other systems.
Telecommunications Access Method (TCAM)	A software protocol which controls the transfer of messages between the application program and the remote terminals and provides the high-level message control language. TCAM's macro instructions can be used to construct programs for controlling messages between several remote stations, or between remote stations and application programs.
Teleprocessing	The processing of data that is received from or sent to remote locations by way of telecommunication lines. Such systems are essential to hook up remote terminals or connect geographically separated computers.
TEMPEST	A government program that prevents the compromising of electrical and electromagnetic signals that emanate from computers and related equipment from being intercepted and deciphered.
Test	Running a program, system, or routine for the purpose of discovering a failure or a potential failure of a program, procedure, or element and to determine its location or potential location.
Test Data	A set of data developed specifically to test the adequacy of computer run or system.
Test Plan	A plan prepared by the government that details the specific tests and procedures to be followed.
Testability	Effort required to test a program to ensure it performs its intended function.
Third-Generation Computer	Any of the computers produced from the mid-1960s to the 1970s that were based on integrated circuits rather than on separately wired transistors.
Threat	Any circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, modification of data and/or software, or denial of service. See also attack.
Throughput	The total measure of useful information processed or communicated during a specified time period.
Time Sharing	The use of a computer system by more than one individual at the same time.

Time Sharing Option (TSO)	A conversational or request/response type of interaction between the system and the individual terminals.
Token	A unique structured data object or message that circulates continuously among the nodes of a token ring and describes the current state of the network. Before any node can send a message, it must first gain control of the token.
Tools	Logical aids to help in constructing solutions to problems.
Top-Down Design	A program design methodology that starts with defining program functionally at the highest level (a series of tasks) and then breaks down each of those tasks into lower-level tasks, and so on.
Top-Down Design Method	Functional decomposition of a problem; that is, gradual progression to levels of greater and greater detail in the development and refinement of a program or system.
Top-Down Programming	An approach to programming that implements a program in top-down fashion. Typically, this is done by writing a main body with calls to several major routines (implemented as stubs). Each routine is then coded, calling other lower-level, routines (also done initially as stubs).
Topology	The configuration formed by the connections between devices on a local area network.
Transaction	A discrete activity within a computer system--usually associated with database management, order-entry, and other online systems. By definition, however, making a deletion or creating a file copy on a microprocessor could as easily be considered a transaction.
Tree	A data structure containing zero or more nodes that are linked together in a hierarchial fashion. The top-most node is called the root. The root is the parent node to its children. Each child can in turn have zero or more children of its own. Every node in a tree has exactly one parent node and all nodes in the tree are descendants of the root node. These relationships ensure that there is always one and only one path from the root node to any other node in the tree.
Trusted Computer System Evaluation Criteria (TCSEC)	A standard of the U.S.-Government for the evaluation of classified computer systems. Synonymous with Orange Book.

Turnkey System	A system in which the manufacturer takes full responsibility for complete system design and installation and supplies all necessary hardware, software, and documentation elements.
Unbundled	Not included as part of a complete hardware/software package.
Unbundled	A pricing strategy in which the services, programs, training, etc., are sold independently of the computer hardware by the computer hardware manufacturer.
Uniform Contract Format	The format required by the FAR for preparation of a solicitation.
Uninterruptible Power Supply (UPS)	An alternative source of power that takes over the job of supplying power to a computer system when regular electrical power fails to permit orderly shutdown of the computer.
UNIX	A type of microcomputer operating system.
Update	As a verb, to change a system or a data file to make it more current. As a noun, a new release of an existing software product.
Upgrade	As a verb, to change to a newer, usually more powerful version. As a noun, the new or enhanced version of a product.
Uptime	The amount or percentage of time a computer system or associated hardware is functioning and available for use.
Use	A major phase of the system's life cycle. The system is put into service.
User	Any person or process interacting directly with a computer system, its information, and/or its assets.
User Friendly	An adjective meaning easy to learn and easy to use.
User Interface	The portion of a program with which a user interacts.
User Management	The management of a specific user area. User management originates work requests, evaluates work, and participates in certain project activities. The user is normally the sponsor of a project who assumes the costs of a project. Another synonym for user is client.
User Profile	A computer-based record maintained about an authorized user of a multiuser computer system.

User Requirements	The functions to be performed by the system. Adequately defined and technically feasible user requirements are important for successful software development.
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	A relative measure of being sound, correct, and efficient. A validity check on data ascertains the degree of accuracy of its representation in a computer.
Validity Checking	The process of analyzing data to determine whether it conforms to certain predefined parameters of completeness and consistency.
Value-Added Network	A communications network that offers additional services besides communications connections and data transmission. Types of value-added services include message routing, resource management, and conversion facilities for computers communicating at different speeds or using different codes or protocols.
Verification	(1) The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase, and (2) formal proof of program corrections.
Verify	To ascertain either that a result is correct or that a procedure or sequence of operations has been performed.
Version	A cycle in the evolution of a system. New versions result from changes in user requirements.
Virtual	An adjective used to describe a device or service that is perceived to be what it is not in actuality. For example, a computer user can treat a virtual disk as if it were a physical disk, but a virtual disk is actually a portion of the computer's memory. Another example is virtual memory, which is stimulated by paging, caching and disk storage.
Virtual Telecommunications Access Method (VTAM)	A software protocol residing in the IBM System 370 series of hardware that gives the remote terminal users access to applications programs. It also provides resource sharing, a technique for efficiently using a network to reduce transmission costs.

Vulnerability	A weakness in security policy, procedures, personnel, management, administration, hardware, software, physical layout, organization, or other factors affecting security that may allow harm to an information processing system. The presence of a vulnerability does not in itself cause harm; a vulnerability is a condition or set of conditions that may allow the information processing system to be harmed by a threat.
Walkthrough	A peer group review of a product or design. A "structured" walkthrough is a walkthrough conducted according to specific rules.
Warnier/Orr Diagram	Structure diagrams for dealing with complex situations. Warnier/Orr diagrams show the relationship of logical conditions among the various modules within a diagram, allowing the user to describe complex logical ideas explicitly within the diagram. Originated by Jean-Dominique Warnier and Kenneth T. Orr.
Warnier-Orr	A hierarchical, structured systems analysis methodology that uses data structure diagrams, program diagrams, in-out diagrams and assembly line diagrams. The structured design method begins at the end or output and works backward.
Wide Area Network	A communications network that connects geographically separated areas.
Wide Area Telecommunications Service (WATS)	A service provided by telephone companies which permits a customer by use of an access line, to make calls to or receive calls from telephones in a specific zone on a dial basis for a flat monthly charge.
Wide Area Telephone Service (WATS)	A telephone company service that permits a customer to dial station-to-station calls via an access line to specific zones for a flat monthly charge, or to receive collect calls in specified numbers at a flat monthly charge rather than on a per-call basis.
Word Processing (WP)	The transition of a written, verbal, or recorded word to verbal, typewritten, or printed form through some form of storage medium that permits the information to be manipulated conveniently before it is committed to final copy.

Work Load	The mix of tasks typically run on a given computer system. Major characteristics include input/output requirements, amount and kinds of computation, and computer resources required.
Yourdon	A method of structured systems analysis and design formalized in 1978. The final product of Yourdon structured analysis, the structured specification, consists of three related components: data flow diagrams, process narratives, and a data dictionary.

BLANK PAGE

Worksheets

The following pages contain sample worksheets that could be used to track the progress of SAF audit tasks. Each table list the audit tasks for a segment, along with a column for a brief summary of the results of the task (e.g., findings) and a column to indicate how the results are supported.

It is suggested that these samples be used as a starting point for the development of more specific worksheets. To do this, obtain the electronic version of these worksheets. Those audit tasks that are not being performed can then be easily removed from the tables.

1.1.1 Scope, Definition, and Organization Segment	Results	Support	Index
Following the agency profile steps, compile and document appropriate background information, including current status of the IRM environment pertinent to the agency program or activity to be audited. Current status information would include major information flows (data and reports) between information providers and information users and other information products and services supporting program goals and objectives.			
Following the agency profile steps, review the report literature--i.e., congressional, prior GAO, inspector general, internal audits, and Financial Integrity Act reports related to the program or activity and identify problem areas pertinent to the review.			
Assess the agency's business plan (this may be their mission plan, management plan, budget document, etc.) to determine: whether the agency identified the stated agency missions, goals, and objectives (of the activity or program to be audited); whether goals and objectives are consistent with the agency's legislated mandates; whether the agency has evaluated its business area and examined or developed new ways to address it's core business issues; whether business area analyses have affected the IRM strategy and action plan; and whether the agency has identified performance measures that will be used in assessing program effectiveness.			
Assess the capability of the agency's planning organization. This can be done by obtaining information on: the composition and skills of the planning team and whether agency executive management considers the mix and number of personnel to be adequate and appropriate; whether the team members have prior experience in performing planning activities and whether they have been successful in the past; whether agency executive management has established a planning effort including senior representatives from user, policy, and IRM organizations affected by the plan; whether the IRM planning charter ensures that (1) agencywide missions, goals, and objectives are properly reflected and incorporated into the planning process, (2) subagency-level plans are sufficiently comprehensive and complete, (3) subagency-level plans are not redundant or overlapping, and (4) the agencywide plan, once approved, is implemented as scheduled.			
Does the agency have policies and procedures for integrating IRM plans with agencywide business plans. (This integration might involve a two-step process, i.e., combining all subagency level IRM plans into an overall IRM plan, and then ensuring that the overall IRM plan is supportive of the agency-wide business plan.) Alternately, does the agency use information engineering methods for integrating information strategic planning with business area analysis with business and technical designs? Make a judgmental assessment of the integration process by looking for anomalies and inconsistencies in the application of these policies and procedures.			

1.1.2 Status and Opportunity Segment	Results	Support	Index
Determine whether the agency has identified the constraints of the external environment, review the agency's documentation of the impact of the external environment on mission performance			
Interview officials to determine whether the agency (i.e., IRM, program, OA, IG, or other unit) has assessed and documented the strengths and weaknesses of its IRM management practices and operations, obtain and evaluate documentation for all assessments made by the agency			
Determine whether the agency has adequately and clearly defined the IRM objectives to satisfy information needs in support of agency mission, goals, and objectives; review the agency's documentation to determine if the objectives are clearly and adequately stated and appropriately linked to mission performance			
Determine whether the agency has assessed the strengths and weaknesses of its overall technological capability (by looking at the level of sophistication, adequacy to meet current user demands, and agency internal surveys), review the agency's documentation to determine the adequacy of its assessment			
Determine whether the agency has identified and documented major technology and functional trends and new opportunities for (a) using information technology, (b) reengineering functions and processes, or (c) using other resources to improve mission performance. If not, why not?			
1.1.3 IRM Strategy Segment	Results	Support	Index
Review the agency's plans and related planning documentation and assess whether the agency (1) established governing strategies for identifying and managing information resources within the agency, including agencywide IRM goals, overall assumptions, and constraints, and (2) provided these strategies to program-level units for their use in developing their components of the IRM strategic plan			
Determine whether the executive management and the designated IRM official have reviewed and approved strategic plan submissions by the subagency-level units to ensure compliance with the strategies and agencywide goals			
Determine whether the strategic IRM plan includes the following critical elements: a mission statement for major functions and operations, general goals and objectives and how they are to be achieved, operational resources (including IT) required to meet the goals and objectives, a schedule for implementing proposed new program initiatives and a description of the organizational and operational impacts of these initiatives, performance goals and measures, an architectural framework, key external factors that could affect the achievement of goals and objectives, and a schedule for future program evaluations and planning adjustments.			
Review the agency's IRM strategy and strategic plan and decide whether it can drive decision making for investing in future information resources needed to accomplish agency mission, goals, and objectives			
Determine whether the IRM strategic plan is linked to the agency's budget, including preliminary program-level IRM budgets			
Determine whether the IRM strategies adequately consider what must be done to transition smoothly from the old IRM environment to the new			
Determine whether senior management has reviewed and approved the IRM strategy and strategic plan			

1.2.1 Scope, Definition, and Organization Segment	Results	Support	Index
Following the agency profile steps, compile and document appropriate background information, including the current status of the IRM environment pertinent to the agency program or activity to be audited. Current status information would include major information flows (data and reports) between information providers and information users and other information products and services supporting program goals and objectives.			
Following the agency profile steps, review the report literature i.e., congressional, prior GAO, inspector general, internal audits, and Financial Integrity Act reports related to the program or activity, and identify problem areas pertinent to the review.			
Assess the agency's strategic IRM plan to determine: whether the agency identified the stated agency missions, goals, and objectives pertinent to the program to be audited, whether program goals and objectives are consistent with the agency's legislated mandates, whether the agency has identified missions and program issues that will impact the IRM operational plan,			
Assess the capability of the agency's planning organization. This can be done by obtaining information on: the composition and skills of the planning team and whether agency executive management considers the mix and number of personnel to be adequate and appropriate, whether the team members have prior experience in performing planning activities and whether they have been successful in the past, whether program management has established a planning effort including program-level representatives from user, policy, and IRM organizations affected by the IRM operational plan, whether the IRM planning charter ensures that (1) agencywide missions, goals, and objectives are properly reflected and incorporated into the planning process, (2) program-level plans are sufficiently comprehensive and complete, (3) program-level plans are not redundant or overlapping, and (4) the agencywide plan, once approved, is implemented as scheduled.			
Does the agency have processes and mechanisms for integrating program-level business and IRM plans and linking them to strategic IRM and agencywide business plans? If yes, make a judgmental assessment by looking for anomalies and inconsistencies in the application of these processes.			

1.2.2 Status and Opportunity Segment	Results	support	Index
Review the agency's documentation and determine whether the agency has effectively identified and described the constraints of its external environment and the impact on its mission and goals.			
Review agency documentation and assess whether the agency has adequately and clearly defined the IRM objectives to satisfy information needs in support of program goals and objectives.			
Interview users/customers, review agency documentation, and assess whether the agency has (a) obtained feedback from the user community on the sufficiency of IRM support to program operations, and (b) clearly identified and articulated user/customer demands for improved information systems and services.			
Interview the user community, review agency documentation, and determine the adequacy of the agency's identification of better ways to use information resources to support program goals and objectives, including opportunities to redesign work processes.			
Review the documentation and determine whether the agency has adequately identified the information products, services, and resources needed to support program goals and objectives.			
Determine whether the agency has identified the strengths and weaknesses of current IRM technical support operations, technical architecture, and capacity and review the documentation to determine the adequacy of the agency's assessment.			
Determine whether the agency has identified the strengths and weaknesses of the IRM organization and review the documentation to determine the adequacy of the agency's assessment.			
Determine if the agency has identified the major information technology trends and the opportunities for using new technology for improved program operations as well as service delivery and review the documentation to determine the adequacy of the agency's assessment.			
Determine whether the agency has documented the criteria for establishing priorities among planned systems development projects, review the documentation and determine whether the criteria are adequate and relevant to program goals and objectives.			
1.2.3 IRM Strategy Segment	**Results**	**Support**	**Index**
Review the IRM operational plan and determine whether it includes an implementation strategy that groups and prioritizes action items into projects that will achieve the IRM objectives, assess the plan for completeness of coverage and depth of implementation details.			
Assess whether the IRM operational plan adequately describes how IRM resources will be used to support program goals and objectives, including an overall architectural framework that supports the selection, use, and integration of information resources within the agency.			
Interview key officials and review agency records to determine whether management reviewed and approved the IRM operational plan, determine whether these officials have properly accepted accountability for implementing the plan.			
Review the plan, budget, and related documentation to determine whether the IRM implementation strategy and operational plan are adequately supported by funding included in the agency's budget, determine whether multiyear funding is likely to be continued for implementation projects to ensure their completion.			
Review the plan and related documentation and interview key officials to determine whether the IRM implementation strategy adequately and systematically considers what must be done to implement the projects and transition smoothly from the old IRM environment to the new.			

2.1.1 Project Initiation Segment	Results	Support	Index
Verify and document that management approval was obtained to initiate the project			
Determine that the project charter was developed and that it describes the project mission and objectives taking into account existing problems, establishes a project team and identifies the person in charge, and shows the specific responsibilities assigned to team members. Verify what the agency did to ensure that the team includes representatives from management, user, and IRM groups that will be affected by the project under development. Specific technical skills of team members should also be described. Evaluate whether the agency team has (1) a thorough understanding of the agency or department's information flow and method of operation, business area, and impediments, 2) produced a document that comprehensively describes the business and system needs that are to be satisfied by the project, and (3) taken a realistic and business-oriented approach to satisfying the objectives of the project.			
Evaluate the background and qualifications of project team members and make a judgment as to whether it was appropriate to assign them to the team. For example, on an Ada software development project it would not be appropriate to assign a software engineer who has no knowledge of the Ada programming language. Further, determine whether the appropriate staff with the necessary skills are represented on the project team. (Note: An information system or computer/communication analyst may be required to assess the qualifications of the team.)			
2.1.2 Project Definition and Scope Segment	**Results**	**Support**	**Index**
Determine whether the project team has scoped the project and developed a system concept that links to business objectives, will improve performance or service goals, and correct known deficiencies. Verify whether the system concept was selected after an evaluation of alternative conceptual approaches. Verify that users agree with the scope and system concept.			
Obtain and evaluate all the cost- and schedule-related documents created in this segment. Determine whether the underlying assumptions, the life-cycle cost estimates and the preliminary cost/benefit analyses are reasonable considering the uncertainty in the system design and organizational barriers and impediments to change, and that estimated benefits are achievable. Expert opinion will be required to help with this analysis.			
Determine if a technical feasibility study and risk assessments exist. With assistance from a technical specialist assess the accuracy, completeness, and reasonableness of these documents. If any of these documents are unavailable, obtain the agency's rationale for this condition.			
Determine whether agency management has monitored the progress and reviewed the documents developed in this segment. Verify that management and users understand the technical feasibility of the project and its associated risks. Finally, verify that management has approved the project's scope and system concept.			
Determine that management has obligated sufficient funds to initiate the project and see it through to completion.			

2.1.3 Work Plan, Standards, and Project Organization Segment	Results	Support	Index
Verify that a work plan and controls for monitoring the project were established. Make a judgment as to whether the schedule, milestones, and monitoring and controlling process are reasonable.			
Assess whether standards have been adopted for the project. Independently verify that the adopted standards are consistent with generally accepted standards and practices used within the agency. Expert opinion may be required to perform the analysis.			
Verify that the project team developed an organizational structure for the project. Verify that the structure identifies the departments within the agency that will be involved in the project, the person responsible for completing the project's design, and the kind of resources that will be needed to complete the project.			
Determine whether users have reviewed the work plan and, adopted standards and an organizational structure for designing the project and agree with them.			
Interview management and obtain verification that they have reviewed and approved the documents developed in this segment and agree with the approach proposed by the project team.			
2.1.4 Management Review and Approval Segment	**Results**	**Support**	**Index**
Determine whether the project team completed and submitted its report (or similar documentation) to agency management for review and approval. Verify that the user and IRM organizations reviewed the project team's report and agreed with its contents.			
Determine whether management reviewed the project team's report, approved the project, and authorized the project team to proceed to the design and development phase. Document this action.			

3.1.1 Needs Identification and Design Segment	Results	Support	Index
Identify projects that haven't yielded a completed product (i.e., a working set of computer programs or an information product such as a report).			
Identify unrealistic costs and schedules that were estimated using ad hoc methods. Verification of costs and schedules may be required using formal tools such as COCOMO or SLIM.			
Determine whether sufficient documentation was developed for a prototype that was subsequently used in an interim production environment.			
Identify ambiguous prototype objectives. Determine if the prototype was approved by management.			
Identify a vague delineation definition of the responsibilities between the IRM organization and the user organization.			
Determine whether the agency performed a business area analysis prior to choosing a particular design model.			
Review the agency's rationale for selecting the iterative approach. The rational should be based on risk aversion.			
Review the agency's technical alternatives analysis. If the analysis is deficient in one or more of the following areas, then the deficiencies should be regarded as potential findings. incomplete, vague, not traceable to agency's mission or goals, unduly restricted options considered, automates existing processes without considering improvements in product or service quality, and unsupportable (i.e., makes unsubstantiated claims or draws unconvincing conclusions).			
Obtain and review the agency's documentation and analyses that demonstrate that the design specification is consistent with the functional and operational requirements.			
Verify that the agency has a risk management plan that identifies risks associated with personnel, cost, schedule, technology, and any other unique features that could jeopardize the project's success.			
Verify that the project management team consistently applied accepted standards and criteria for system design.			
Determine whether the appropriate number of staff, personnel skills, training, tools, and computing resources are available to the project team.			
Obtain and review documentation (conversion or reengineering plan) describing how the agency will transition to the new system with minimal disruption.			
Evaluate the RFP or similar solicitation documents for anomalies, inconsistencies, and restrictiveness.			
Verify that the agency's quality assurance and control functions have been exercised appropriately in this segment.			

3.1.2 System Development and Deployment Segment	Results	Support	Index
Review the agency's documentation to determine whether the detailed designs, code, and test results are completely documented			
Determine if cost and schedule estimates, resource requirements, and performance specifications have been updated and documented			
Review the thoroughness of the agency's validation and verification process and verify with the user organization whether the system satisfies the functional and operational requirements of the users (i.e., are 90% of all prescription orders filled at army hospital X completed in 10 minutes or less?) If not, why not?			
Review the updated risk analyses and assess whether the agency's analysis is reasonable			
Verify that the project management team consistently applied accepted standards and criteria in building the system.			
Evaluate whether appropriate skills and resources were available and used in this segment			
Obtain and evaluate the RFP or similar solicitation documents for (1) completeness, (2) traceability to the agency concept of operations and mission goals, and (3) consistency			
Determine whether the agency used the experience it gained in iteratively developing the system to improve or change its operations (i.e., lessons learned)			
Determine whether agency policies and procedures were followed for installing the system and whether the installation occurred with minimal disruption to the user and normal business operations			
Verify with management that the installed system is meeting the agency's mission needs.			
Ensure that management approved moving into the next segment.			
3.1.3 Review Segment	**Results**	**Support**	**Index**
If the project has not been abandoned, review updated cost and schedule and determine whether expended resources have been recorded properly and warrant proceeding with the project.			
Determine whether the risk analyses provide a sound basis for continuing or abandoning the project and check this against the agency's decisions			
Verify that the agency has (1) developed a system that meets user functional and operational requirements including performance expectations, (2) formally approved the system to transition to operational status; (3) documented the need for additional enhancements and approved continuing development iterations, or (4) documented its decision to abandon the system.			
Verify that the project team consistently applied accepted standards and criteria such as quality assurance, configuration management, and security in meeting its objectives.			
Evaluate the RFP or similar solicitation documents for traceability of functions in the completed system to the requirements in the RFP			
Verify that the agency used lessons learned in the iterative process of developing the system			

3.2.1 Needs Identification Segment	Results	Support	Index
Determine that the user's functional and operational requirements were appropriately derived using conventional techniques such as business area analysis, etc.			
Assess whether the user requirements document is unambiguous, complete, verifiable, consistent, modifiable, and traceable (ANSI/IEEE Standard 830-1984)			
If the agency has established the use of software development tools, obtain the agency's guidelines for using such tools and determine whether both guidelines and these tools were used for developing the user requirements.			
Identify the unique features that contribute to high risk of failure in identifying user requirements and assess whether agency management has taken steps to address these in the risk management plan. If no, then this is a finding.			
Evaluate sensitivity analyses for approximate costs and schedules.			
Verify that management consistently applied the agency's internal controls, generally accepted standards and criteria in meeting the objectives of this segment.			
Independently analyze cost and schedule reports using cost estimation tools such as COCOMO, COSTAR, or SLIM to verify that the reported costs and schedules are similar to those derived using these tools.			
Determine whether appropriate staff, skills, and computing resources were available to the project team.			
Verify that the entity obtained management approval before proceeding to the next segment.			
Evaluate solicitation documents for anomalies, inconsistencies, and reasonableness.			
3.2.2 System Design Segment	**Results**	**Support**	**Index**
Draw a sample from the overall system specifications and trace them back to supporting functional and operational requirements. As a short cut, agency management can be asked for such a document from their quality assurance or oversight group.			
Verify that the risk management plan has been updated per the refinements identified in the system design specification.			
Verify that the agency has evaluated the impact of the system design specifications on the estimated costs and schedule for the program or project.			
Verify agency compliance with applicable policies, procedures, and standards.			
If appropriate, evaluate the quality of the solicitation document.			
Determine whether the technical architecture is consistent with agency's new concept of operations.			
Assess the agency's system design for ambiguities, completeness, consistency, maintainability, robustness, traceability, and usability.			
Verify that adequate consideration was given to continuity of operations (i.e., disaster recovery, routine outages, etc.) for key user processes.			

3.2.3 System Development and Deployment Segment	Results	Support	Index
Obtain updated organizational charts			
Determine whether relevant program and project management plans have been updated. These plans should include updated cost estimates, schedules, and tasks.			
Verify that the agency complied with the relevant federal laws, regulations, and standards, as well as agency specific policies, procedures, and standards.			
If appropriate, evaluate the quality of the solicitation document.			
Verify that program and project risks were reduced through the use of conventional system development tools (i.e., computer aided design (CAD), computer aided software engineering (CASE), and fourth generation languages) and techniques (i.e., peer reviews, structured walkthroughs, formal inspection, etc.)			
Obtain the overall system design document and the detailed system, subsystem, module, computer program, or database specifications, if required.			
Evaluate the agency process for the acquisition of commercial-off-the-shelf (COTS) products (i.e., computer equipment, communications equipment, and software). Verify that the products acquired are supported by the system architecture, design, and operating characteristics. Also verify that system integration issues associated with COTS products have been resolved.			
Evaluate the impact (i.e., technically, operationally, and financially) of agency modifications to COTS products. Verify that the modifications were properly documented and communicated to management.			
Evaluate the agencys' software engineering processes for critical attributes (i.e., key process areas) such as software configuration management, software subcontract management, and software quality assurance. Note: Consult with the chief scientist for assistance from a software capability evaluation(SCE) team.			
Verify that testing was done in accordance with the test plan approved by agency management.			
Verify the existence and evaluate the adequacy of the various planning documents (i.e., transition plan, training plan, deployment plan, etc.) produced during development and deployment.			
Verify that the agencys' derivation of the estimated costs and schedule is reasonable (i.e., supportable through the use of tools, deductive logic, conventional industrial cost estimating techniques).			

3.2.3 System Development and Deployment Segment (continued)	Results	Support	Index
Verify that the detailed design contains no anomalies or inconsistencies relative to the technical and functional specifications developed during the Design segment.			
Verify that plans for testing and conversion were developed during this segment. Evaluate these plans for accuracy, completeness, and realism.			
Verify the results of the various levels of testing (i.e., unit, integration, or system) for consistency with performance requirements defined during the System Design segment. This would include concerns such as (1) system response time, (2) peak workload (i.e., stress) processing, and (3) operational performance sensitivity to the choice of language or database characteristics.			
Obtain a copy of various test analyses reports, if available.			
Verify that a thorough and complete verification and validation of the system developed in this segment was done by the agency.			
Evaluate the operational readiness of (1) the system, (2) the user environment to receive the system, and (3) the operational and maintenance support environment for the system. Operational readiness issues include (1) the resolution of all critical and most high-priority system problem reports, (2) completion of initial training for the first group of users to receive the system, and (3) establishment of a rigorous hardware and software configuration control process for sustainability (i.e., overall system maintenance and support).			
Evaluate the effectiveness of the agencys' conversion from the legacy environment to the new system. Check for (1) the accuracy and completeness of the data conversion, (2) revisions and replacements of old procedures, (3) training and indoctrination processes for users of the new system, etc.			
Evaluate the reasonableness of contingency plans.			
Evaluate the impact of managerial decisions throughout the development and deployment of the system. Also focus on the continued affordability of the system.			
Evaluate the existence and determine the adequacy of operationally oriented performance measures for the programmatic area(s) affected. In lieu of performance measures, agencies may periodically perform benefit realization studies, program evaluations, in-process reviews, etc.			

4.1.1 Day-to-Day Operations Segment	Results	Support	Index
Review the agency and system profiles and update them if necessary. Verify that the computer equipment, system software, communication equipment, communications software, production job streams, cataloged applications, hardware configuration, network topology, and overall system architecture is documented and understood by the evaluation team.			
Identify the internal & external information flows, services, and products that are critical to the success of the federal program or activity under study and assess whether the system effectively supports these flows, services and products. Ask for customer support agreements, periodic operational performance reports against predetermined operating goals, system incident reports, etc.			
Determine whether the agency is maintaining unofficial or unauthorized ("cuff") records to fulfill their information needs because current systems are ineffective.			
Identify deficiencies and ask users how the system could better support their needs.			
Determine whether the agency has established problem-management procedures. Obtain examples where operational problems have occurred, and determine whether the problems (1) were resolved within the system or procedurally (i.e., a temporary workaround solution); and (2) caused any adverse effects on system operations, user satisfaction, or the attainment of program objectives.			
Determine whether appropriate controls have been established to mitigate risks. For example, has the agency taken into account the feasibility or learning curve of moving from contractor operated systems in the new environment to government-operated systems with individuals who have little or no experience in the new environment.			
Verify the stability of the system support facilities. Addresses issues such as the adequacy of the power supply, air conditioning, humidity control, etc.			
Verify that the agency's continuity of operations plans are up to date and periodically tested.			
Evaluate that training programs adequately maintain skill levels for operations personnel.			
Make a general assessment as to whether the agency is operating and managing day-to-day operations in compliance with policies, standards, procedures, and applicable laws and regulations.			
4.1.2 System Measurement and Evaluation Segment	**Results**	**Support**	**Index**
Review service-level agreements between users and IRM support staff and verify that they are being fulfilled.			
Verify that agency analyses of system responsiveness, availability, and reliability are accurate and complete.			
Verify that the results of agency tests for continuity of operations are accurate and complete.			
Verify that controls have been tested by the agency to ensure that (1) the system produces accurate, complete, reliable, and timely information to users; and (2) the system is protected against unauthorized access, accidental loss, fraud, waste, abuse, and mismanagement.			
Determine whether an effective security awareness program is operational and that agency personnel are properly trained in matters relating to security.			
Verify that the agency is managing its operations in compliance with policies, standards, procedures, and applicable laws and regulations.			

4.2.1 System Configuration Management Segment	Results	Support	Index
Interview both agency and program management to obtain policies and procedures that cover system change control and their expectations regarding expected usage within the organization.			
Review the policies and procedures to verify that the change control policies and procedures exist and are both internally consistent and consistent with other agency policies.			
Evaluate current practices within system operations and the user organizations to determine the degree of consistency between these practices and current policy.			
Review the change request log, if any, for completeness, existence of anomalies, and inconsistencies.			
Confirm that system operations and user group change requests are formally received, logged, classified, and prioritized.			
Determine the reasonableness of the process the agency used to estimate (1) cost and time to implement the changes logged and (2) the impact on the system.			
Review the prioritization process, examining specific change requests and their assigned priorities. Determine whether anomalies and inconsistencies exist in the prioritization process.			
Evaluate the reasonableness of priorities.			
Interview users to determine whether they are satisfied with the priorities assigned to change requests.			
Verify that the disposition of system change requests is communicated to the requesting individual or organizational entity.			
4.2.2 System Modification Segment	**Results**	**Support**	**Index**
Review system change requests to determine if the disposition of the requests was determined in an expedient manner. Determine the role that priority setting played in this process.			
Evaluate the adequacy of the system and software engineering practices used in implementing the approved changes.			
Examine the technical standards and tools used in design and development such as software configuration management tools, reliability assessment models, and project management and system development software tools and assess the quality of the system development environment.			
Review the user documentation (procedures, manuals, on-line help, etc.) to determine whether this documentation clearly and accurately reflects the change request.			
Interview QA personnel and users to verify that hardware and software changes were adequately tested using policies and procedures established by the agency.			
Evaluate the agency's actual costs and schedule against the various estimates produced during the modification and inquire as to what adjustments the agency intends to make to its estimating process to improve in the future.			

Index

BLANK PAGE