

July 1986

Evaluating the Acquisition and Operation of Information Systems

Preface

The federal government is becoming increasingly dependent on information technology to meet its mission and program goals, presenting new challenges for the audit community. Collectively, the government is the single largest user of information technology in the world and spends billions of dollars annually on its information resources--hardware, software, data, and people. This growing reliance on information technology emphasizes the need to economically acquire, develop, operate, and maintain information resources to effectively and efficiently achieve agency mission and objectives. The Information Management and Technology Division (IMTEC) is the General Accounting Office's (GAO) focal point for evaluating how well the government manages its substantial investment in information resources.

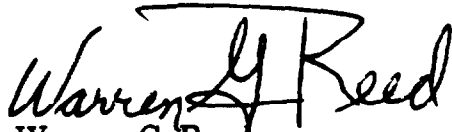
This guide provides GAO and IMTEC staff, as well as other interested officials in the federal audit community, with a logical framework for evaluating government agencies' acquisition and operation of computer-based information systems. It is structured around a matrix that outlines two broad information system life cycle phases--acquisition/development and operation/maintenance--as they relate to five basic objectives. As described in the guide, agencies should achieve the following objectives in acquiring and operating their information systems:

- Ensure system effectiveness.
- Promote system economy and efficiency.
- Protect data integrity.
- Safeguard information resources.
- Comply with laws and regulations.

The guide also provides general criteria for evaluating agencies' performance in achieving these objectives by highlighting key practices that should occur during the system life cycle. The appendix is a convenient reference to the most significant laws, regulations, and standards that affect the federal information processing environment.

This guide supplements and does not replace any other GAO policies or procedures. It may be updated as necessary.

I hope that IMTEC staff and other users of this guide will find the framework presented here beneficial in performing their work. It should help us meet the audit challenge of ensuring that federal policies and procedures foster good information management, and that agencies maximize the return on their information technology investment.



Warren G. Reed
Director, Information Management
and Technology Division

Contents

Preface

1

**Chapter 1
Role of the Guide in
Information System
Evaluations**

Organization and Content of the Guide
Using the Guide

6
6
7

**Chapter 2
Underlying Concepts**

Information System Definition
Information System Life Cycle
The Five Basic Objectives
Relationship Between the Life Cycle and
the Five Basic Objectives
Agency Practices to Achieve the Five Basic
Objectives

8
8
8
11
12
14

**Chapter 3
System Acquisition/
Development--
Practices to Meet the
Five Basic Objectives**

Environmental Practices Lay Foundation for
Meeting the Five Basic Objectives
Strategic ADP Management Practices
Tactical ADP Management Practices
Specific Practices Aid in Evaluating Acquisition/
Development Projects
Requirements Definition
Analysis of Alternatives
Acquisition Process
Software Engineering
Environmental and Specific Practices Help
Achieve the Five Basic Objectives
Ensuring System Effectiveness
Promoting Economy and Efficiency
Protecting Data Integrity
Safeguarding Information Resources
Complying with Laws and Regulations

16
16
16
18
19
20
20
20
21
21
21
23
24
25
25

Chapter 4		27
System Operation/ Maintenance-- Practices to Meet the Five Basic Objectives	<ul style="list-style-type: none"> Environmental Practices Help Agencies Achieve the Five Basic Objectives 27 <ul style="list-style-type: none"> Data Center Operations 27 Capacity Management 29 Telecommunications Management 29 Data Center Security 30 Specific Practices Focus on Individual Application Systems 30 <ul style="list-style-type: none"> Application Control Framework 31 Environmental and Specific Practices Help Achieve the Five Basic Objectives 34 <ul style="list-style-type: none"> Ensuring System Effectiveness 34 Promoting Economy and Efficiency 34 Protecting Data Integrity 36 Safeguarding Information Resources 38 Complying with Laws and Regulations 39 	27
<hr/>		
Chapter 5		40
Crosswalk to Additional Guidance	<ul style="list-style-type: none"> Linkage Between the Guide and GAO's Job Management Framework 40 Linkage Between the Guide and Available Criteria 41 	40
<hr/>		
Appendix		42
The Compliance Objective--Key Laws, Regulations, and Standards	<ul style="list-style-type: none"> Laws, Regulations, and Directives 42 OMB Circulars 45 GAO Standards 46 Federal Information Processing Standards Publications (FIPS PUBs) 48 	42
<hr/>		
Tables	<ul style="list-style-type: none"> Table 2.1: Key Activities in the Information System Life Cycle 10 Table 2.2: Relationship Between the Five Basic Objectives and the Information System Life Cycle 13 Table I.1: Key Laws, Regulations, and Directives--Relationship to the Other Information System Objectives 44 Table I.2: Key OMB Circulars and GAO Standards--Relationship to the Other Information System Objectives 47 Table I.3: Key FIPS PUBs--Relationship to the Other Information System Objectives 51 	10

Figures

Figure 2.1: Structure of the Guide--Chapters 3 and 4 Show Relationship Between Key Practices and the Five Basic Objectives

Abbreviations

ADP	automatic data processing
DOD	Department of Defense
FIPS PUBs	Federal Information Processing Standards Publications
FIRMR	Federal Information Resources Management Regulation
GAO	General Accounting Office
IMTEC	Information Management and Technology Division
NSDD	National Security Decision Directive
OMB	Office of Management and Budget

Role of the Guide In Information System Evaluations

As the focal point for the General Accounting Office's (GAO) data processing and telecommunications work, the Information Management and Technology Division (IMTEC) evaluates policy, management, and technology issues on an agency-specific and a governmentwide basis. Auditing system acquisitions and operations at individual agencies consumes the bulk of IMTEC's staff resources and lays the foundation for identifying and assessing governmentwide issues and problems. IMTEC's primary goal in performing this work is to determine if agencies are making sound managerial, technical, and economical decisions in acquiring and using automated systems.

To help achieve our goal, this guide provides a logical framework for evaluating system acquisitions and operations. More specifically, it is intended to

- direct and focus IMTEC's agency-specific work;
- guide staff in defining, planning, and communicating audit objectives; and
- provide a consistent structure for developing governmentwide issues.

While the guide does not describe in detail the exact tasks required to perform an audit, it does provide parameters for our work by (1) defining objectives agencies should achieve in acquiring and operating computer-based systems and (2) highlighting some key criteria for measuring agency performance in meeting the objectives.

Organization and Content of the Guide

The chapters of the guide follow a logical sequence--from broad concepts and management issues to more specific system life cycle phases and the respective agency practices that should be in place. Following this introductory chapter, chapter 2 describes some fundamental concepts that form the backbone of this guide: our definition of a computer-based system and its life cycle; a description of the five basic objectives that agencies should meet in acquiring and operating these systems; and a definition of the key categories of practices, or internal control techniques, that are important to achieving the five objectives.

The remaining chapters show the relationship between the life cycle phases and each of the five objectives, highlighting key

practices that should be performed. Chapter 3 provides an overview of the system acquisition/development life cycle phase and the practices needed to meet each of the five basic objectives, while chapter 4 provides similar information on the system operation/maintenance life cycle phase. The final chapter links the guide to GAO's job planning and management process and to available criteria.

Using the Guide

We intend for this guide to be used primarily by GAO staff responsible for auditing data processing and telecommunications issues at specific agencies and across the government. However, it may also prove useful to individuals outside GAO, including agency internal audit staff, inspectors general staff, and electronic data processing managers and personnel involved in developing and operating information systems.

The guide provides broad parameters for determining whether computer-based systems meet or will meet five basic objectives. It familiarizes auditors with the various phases of the life cycle process and allows flexibility for zeroing in on the applicable life cycle phase of the system under review. This guide should be particularly useful early in the audit process, in establishing audit objectives, identifying potential problem areas, and determining the scope and extent of more detailed audit work.

Underlying Concepts

To place the information in this overview guide in its proper context, some fundamental concepts need discussion. These concepts include (1) the definition of a computer-based system, (2) the life cycle of a system, (3) the five basic objectives that should be considered in evaluating the system, (4) how the basic objectives will change during the system life cycle, and (5) the categories of agency practices that are necessary to achieve the basic objectives.

Information System Definition

A computer-based system (hereafter referred to as "information system") is the product of four basic information resources-- hardware, software, data, and people--combined into automated and manual steps or processes to accomplish a specific organization mission or objective. This "total system" definition includes the automated and manual functions of input, communications, processing, storage, and output. Under this definition, for example, an information system performs certain processes, or applications (e.g., tracking the movement of air traffic, compiling economic statistics), to help accomplish a specific objective (e.g., preventing airplane accidents, monitoring the nation's economic growth).

Information System Life Cycle

An information system has a basic life cycle that begins with its acquisition and/or development and continues through its operation and maintenance. For IMTEC's purposes, an acquisition is defined as (1) procuring (i.e., contracting out or purchasing) computer hardware and/or software off the shelf, and/or (2) procuring hardware and/or software development services from external contractors. Development is defined as designing, building, or modifying hardware and/or software to meet an organizational need. Our definition of the system operation/maintenance life cycle phase is relatively straightforward--an operational system currently performs certain functions to meet an organizational need, while system maintenance involves changes or adjustments to keep the system functioning as intended.

Both of these broad life cycle phases can be broken down into smaller phases, each of which has several steps or activities. Table 2.1 identifies the major categories of the information system life cycle and lists some of the key activities that should

generally occur. Chapters 3 and 4 of this guide provide insights into these categories and activities.

A structured information system life cycle process with action-oriented phases assists agencies in managing the design, implementation, and maintenance of computerized systems. By providing an organized approach to system acquisition/development and operation/maintenance, it also guides auditors in evaluating agency practices. While the terminology for the phases may differ from one agency to another, the actual process is fairly consistent and facilitates monitoring and assessing an information system's management, development, and performance at critical points.

Table 2.1: Key Activities in the Information System Life Cycle

SYSTEM ACQUISITION/DEVELOPMENT	
<u>System Planning and Initiation</u>	
<ul style="list-style-type: none"> ● Prepare long-range strategic automatic data processing (ADP) plan consistent with agency needs. <ul style="list-style-type: none"> ● Identify user needs in context of agency mission, resources, and priorities. 	
<u>Requirements Definition and Analysis of Alternatives</u>	
<ul style="list-style-type: none"> ● Define and validate user needs in terms of functional, data, and operational requirements. ● Identify alternatives to meet requirements and analyze technical and operational feasibility. <ul style="list-style-type: none"> ● Estimate and compare costs and benefits. ● Select and approve an alternative and prepare project plan. 	
<p style="text-align: center;"><u>Acquisition Strategy</u></p> <ul style="list-style-type: none"> ● Select acquisition strategy commensurate with cost, risk, and urgency of need. ● Prepare an acquisition schedule. <p style="text-align: center;"><u>Procurement Cycle</u></p> <ul style="list-style-type: none"> ● Prepare solicitation documents, including technical specifications and evaluation factors. ● Select procurement method and contract type. ● Evaluate proposals and award contract. ● Monitor and manage contract. 	<p style="text-align: center;"><u>Design and Development</u></p> <ul style="list-style-type: none"> ● Develop detailed system design, including requirements for output, input, files, data, and controls. ● Prepare validation/testing goals and plans. <p style="text-align: center;"><u>Application Programming and Testing</u></p> <ul style="list-style-type: none"> ● Program from detailed design specifications. ● Test, debug, and document programs. ● Prepare manuals for users, operations, and program maintenance. ● Perform unit tests and document results.
<u>Acceptance Testing</u>	
<ul style="list-style-type: none"> ● Perform acceptance test to determine if system meets requirements. Document test results. 	
SYSTEM OPERATION/MAINTENANCE	
<u>Implementation</u>	
<ul style="list-style-type: none"> ● Modify physical site to accommodate any hardware and install. Change over forms, displays, and files. Train data processing staff and users. Change over to new system. 	
<u>Operation/Maintenance</u>	
<ul style="list-style-type: none"> ● Operate, refine, and fine-tune system, as needed. Perform on-going maintenance. Conduct periodic reviews to determine if changes are warranted. 	

The Five Basic Objectives

For agencies to make sound managerial, technical, and economical decisions in acquiring/developing and operating/maintaining information systems, they need to meet five basic objectives. A brief discussion of each of these five objectives follows.

- **Ensure system effectiveness.** An information system exists to serve some higher need, such as issuing social security checks or providing real-time information on the nation's air traffic. The information that meets this need can take a variety of forms, from daily hard-copy reports to radar screens displaying instantaneous air speed, altitude, and directional information. System effectiveness is measured by determining whether the system performs the intended functions and whether users get the information they need, in the right form, in a timely fashion.
- **Promote system economy and efficiency.** An economical and efficient system uses the minimum number of information resources to achieve the output level the system's users require. Economy and efficiency must always be considered in the context of system effectiveness--they are meaningless if effectiveness is not being achieved. Information systems consume scarce resources--hardware, software, data, and people--which should be optimized in meeting organizational and user needs.
- **Protect data integrity.** To make sound managerial decisions, organizations need properly authorized, complete, accurate, and reliable data. Achieving the data integrity objective requires that systems have adequate controls over how data are entered, communicated, processed, stored, and reported.
- **Safeguard information resources.** An organization's information resources, which include its hardware, software, data, and people, are often concentrated in a specific physical location, e.g., a data or telecommunications center. As with all valuable assets, these resources need to be protected against waste, loss, unauthorized use, and/or fraud.
- **Comply with laws and regulations.** Congress has passed laws, the central executive branch agencies have established regulations, and the individual agencies have defined policies and procedures that govern the acquisition/development and operation/maintenance of information systems. Ensuring

compliance with these laws, regulations, and policies will help achieve the four objectives cited above and will promote federal policy goals.

While auditors should understand the distinctions between each of these five basic objectives, they should also recognize that the objectives are interrelated and need to be carefully balanced in evaluating system acquisition and operation. Achieving one objective could adversely affect meeting another objective. To meet the data integrity objective, for example, an agency would implement certain controls to ensure that the data are accurate, reliable, and complete. Since these controls also have a cost, they affect the agency's ability to achieve the economy and efficiency objective. Further, the most accurate data would be meaningless if it does not promote the system effectiveness objective (i.e., the organization and the system users do not need it).

Relationship Between the Life Cycle and the Five Basic Objectives

The relationship between the information system life cycle outlined in table 2.1 and the five basic objectives defined above is the theme of this guide. As the table indicates, each major life cycle phase is comprised of sub-phases and their related activities. When the five basic objectives are applied to this life cycle process, their focus will shift depending on where the system under review is in the life cycle process. If the system is being acquired/developed, for example, meeting the data integrity objective would involve building adequate controls and audit trails into the system design. Once the system becomes operational, the focus of the data integrity objective will shift to ensuring that the controls function as intended. During system maintenance, the design of adequate controls could again become important with the need to not eliminate any necessary controls in making changes to the system.

The other four objectives will have similar shifts in focus as they are applied to the different life cycle phases. The matrix in table 2.2 relates each of the five basic objectives to the two major system life cycle phases, highlighting the variations that can occur. More detailed discussions of each box in the matrix begin in chapter 3 of this guide.

Table 2.2: Relationship Between the Five Basic Objectives and the Information System Life Cycle

LIFE CYCLE OBJECTIVES	ACQUISITION/DEVELOPMENT	OPERATION/MAINTENANCE
ENSURE SYSTEM EFFECTIVENESS	Acquisition/development contributes to the agency's achieving its mission and objectives. System is acquired/developed to meet user functional and data requirements.	System operates so that it meets the user functional and data requirements established during acquisition/development. Proper maintenance ensures that operational system continues to meet these functional and data requirements.
PROMOTE SYSTEM ECONOMY AND EFFICIENCY	Acquisition/development results in selection of a system that optimizes the number of resources used, while remaining effective.	System operates and is maintained so that it uses the optimum, least-cost mix of resources to meet user functional and data requirements.
PROTECT DATA INTEGRITY	System is acquired/developed with adequate controls and audit trails over data origination, input, communications, processing, storage, and reporting, so that the system will produce accurate, complete, and reliable data.	System controls operate to ensure that data are properly originated, entered, communicated, processed, stored, and reported and, therefore, are accurate, complete, and reliable. Maintenance procedures ensure operational system continues to provide accurate, complete, and reliable data.
SAFEGUARD INFORMATION RESOURCES	Acquisition/development includes adequate organizational and environmental controls to protect resources from waste, loss, unauthorized use, or fraud.	Organizational and environmental controls, designed to protect resources from waste, loss, unauthorized use, and fraud, operate independent of application.
COMPLY WITH LAWS AND REGULATIONS	Acquisition/development process complies with applicable laws and regulations; for example, Brooks Act, Office of Management and Budget (OMB) Circulars. Acquired/developed system conforms to laws and regulations that define agency mission.	System conforms with applicable laws and regulations; for example, Paperwork Reduction Act, Federal Managers' Financial Integrity Act, and Privacy Act.

Agency Practices to Achieve the Five Basic Objectives

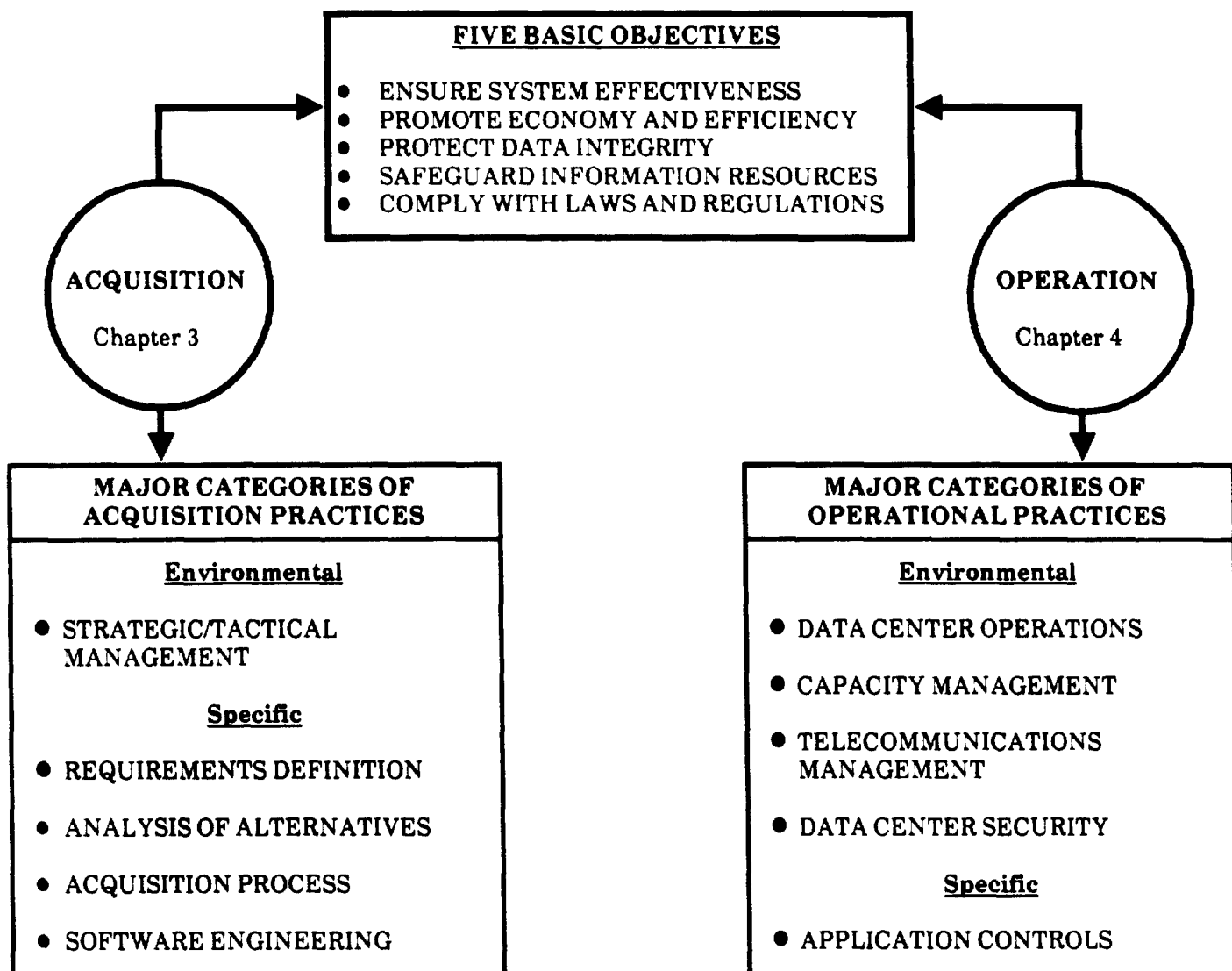
The matrix presented in table 2.2 is the underlying structure for the remainder of the guide. It is supported by agency practices, which serve as the building blocks to achieve each of the five basic objectives during the information system life cycle. Generally, agency practices fall into the following two groups:

- **Environmental Practices.** Environmental practices, which are also known as general or management controls, apply to the environment in which all systems are acquired/developed and operated/maintained. These practices include strategic/tactical management activities, such as ADP planning and budgeting, as well as data center operations, capacity management, and telecommunications management.
- **Specific Practices.** Specific practices apply to individual system acquisition/development projects or to distinct operational information systems and their related maintenance. For example, an acquisition-specific practice could include how user requirements were identified and defined for a particular system. On the other hand, operation-specific practices typically address the functioning of a certain computer application and how well it accepts, communicates, processes, stores, and reports data.

For both life cycle phases, the guide briefly discusses broad categories of agency practices, and then relates key practices from these categories to each of the five basic objectives.

Figure 2.1 provides an overview of the structure and key topics covered in chapters 3 and 4 of the guide. As illustrated in the figure, the matrix can be broken down into the five basic objectives and the two life cycle phases--acquisition and operation. Chapter 3 focuses on the acquisition phase and briefly discusses some broad categories of acquisition practices: strategic/tactical management, requirements definition, analysis of alternatives, acquisition process, and software engineering. Chapter 4 addresses the operation phase and summarizes broad categories of operational agency practices: data center operations, capacity management, telecommunications management, data center security, and application controls. Both chapters close by relating more detailed agency practices from these broad categories to each of the five basic objectives. Figure 2.1 also shows that most of the activities related to an acquisition fall into the *specific practices* group, while most of the activities related to an operational system fall into the *environmental practices* group.

Figure 2.1: Structure of the Guide--Chapters 3 and 4 Show Relationship Between Key Practices and the Five Basic Objectives



System Acquisition/Development-- Practices to Meet the Five Basic Objectives

The practices used in acquiring and developing an information system are important to achieving the five basic objectives and to laying the foundation for subsequent system operation and maintenance. During acquisition/development, environmental and specific practices help ensure that agencies

- acquire/develop systems that meet user requirements;
- select systems that optimize resource use and minimize cost;
- design systems with adequate controls and audit trails;
- protect resources from waste, loss, or unauthorized use; and
- comply with applicable laws and regulations.

This chapter briefly discusses key environmental practices applicable to the acquisition/development life cycle phase, summarizes major acquisition-specific practices, and relates some of these practices to each of the five basic objectives.

Environmental Practices Lay Foundation for Meeting the Five Basic Objectives

By establishing and enforcing environmental practices for planning and managing the acquisition/development phase, agencies can better ensure that their information systems will meet all five basic objectives. The key environmental practices that should be present during acquisition/development are listed below under the broad categories of strategic and tactical ADP management. In evaluating these practices at an agency, auditors should determine whether a structured acquisition/development process exists and whether users, management, and internal auditors have participated in the process.

Strategic ADP Management Practices

High-level, or strategic, agency management has an important role in ensuring that information systems are acquired/developed in a planned and controlled manner. Strategic management typically assumes a top-down flow--agency management establishes certain policies and procedures, assigns responsibility for implementing these policies and procedures to each organizational unit, and holds each unit accountable for executing their responsibilities. Assessing agency activities in the following strategic management areas--agency mission, goals, and objectives; ADP planning and budgeting; ADP organization; ADP personnel; and internal audit--provides insights into the strengths and weaknesses of the acquisition/development environment.

Agency mission, goals, and objectives

Agency mission, goals, and objectives establish what functions the agency should be performing and how it should execute these functions. They are the primary directing force within the agency and should be reflected throughout the organization. These authorities and responsibilities are usually mandated by public laws (i.e., statutes passed by the Congress) and may be affected by executive orders issued by the President.

To direct its objectives and program activities, agencies should generally interpret and condense these statutes and executive orders into mission statements. These mission statements should set out specific objectives for the agency to achieve, and serve as the basis for planning and ranking ADP projects, assigning resources, and evaluating performance.

ADP planning and budgeting

To support the agency in achieving its mission, goals, and objectives, top management should establish a formal ADP planning and budgeting process that identifies organization-wide needs for information systems and lays out long- and short-range strategies for acquiring/developing and operating/maintaining these systems. Representatives from all sections of the organization--users, operations, system design and development, security, senior management, and internal audit (in an advisory capacity)--should actively participate in the ADP planning and budgeting process.

Organization

An agency's organization structure should facilitate implementing its ADP plans and so help the agency achieve its mission, goals, and objectives. To be effective, the ADP function should complement the agency's overall organization and should be positioned high enough in the organizational hierarchy to put it on equal footing with user departments.

One of the most basic organizational practices is separation of duties, which is particularly important in acquiring/developing information systems and in their subsequent operation/maintenance. The principle underlying separation of duties is that one person should not be in a position to commit and to conceal errors and irregularities. In the information system

environment, for example, a computer operator should not participate in system development activities since knowledge of the system's controls would put the operator in an excellent position to circumvent them. In small or highly centralized organizations, where separation of duties is not practical, some form of compensating practices (e.g., access controls and supervisory personnel procedures) should be implemented.

ADP personnel

An agency's personnel practices are important to establishing a sound information system environment. ADP personnel practices include hiring and training of employees, appropriate supervision and work quality standards, vacation and health benefits, and termination policies. Inadequate personnel procedures, or lack of compliance with established procedures, can contribute to low employee morale and high turnover rates--conditions that can lead to an ADP environment characterized by carelessness, errors, and omissions.

ADP audit

Internal and/or external ADP auditors should review information system acquisition/development projects to provide agency management with reasonable assurance that auditable and properly controlled systems are being acquired/developed. According to GAO's Standards for Audit of Governmental Organizations, Programs, Activities, and Functions (1981 Revision), the auditor should not become part of the system acquisition/development team, but should review the team's work as it occurs, suggest audit trails or other control practices to the team, and give management an objective evaluation of the team's work. Throughout the acquisition/development phase, auditors should also consider the agency's compliance with the five basic objectives presented in this guide.

Tactical ADP Management Practices

While strategic management practices provide long-term direction for acquiring/developing information systems, tactical management practices establish the environment for the agency's day-to-day acquisition/development activities. A standard information system life cycle with action-oriented phases is an important tactical management tool. By following

a life cycle process like the one outlined in table 2.1, management can help ensure that information systems are acquired/developed on schedule, within costs, and to the users' satisfaction.

Project management and documentation are key environmental practices that should be inherent in the agency's life cycle process. A brief description of each of these tactical management practices follows.

Project management

A formal project approach for acquiring/developing information systems can help top management ensure that the life cycle process is successfully implemented. The objective of project management is to provide a structured means for measuring progress in acquiring/developing an information system. Some key project management practices include developing a project plan, budget, and schedule; preparing project status reports and establishing intermediate work products; directing and leading a project team; interfacing with users and the ADP planning group; and monitoring project execution, including actual versus budgeted expenditures and actual versus scheduled completion dates.

Documentation

Adequate documentation of the various project phases is essential to the system's acquisition/development and its subsequent operation/maintenance. Documentation is an orderly process of defining and describing the system's goals, functions, and development. During the acquisition/development life cycle phase, documentation also promotes more accurate communication between project managers, end users, and other project participants (e.g., contractors, system analysts, and programmers).

Specific Practices Aid in Evaluating Acquisition/ Development Projects

A basic understanding of specific acquisition/development practices is important to evaluating an agency's progress in achieving the five basic objectives. In contrast to broad environmental practices that have an organization-wide impact, specific practices are meaningful primarily at the acquisition/development project level. Brief summaries of

these specific practices--requirements definition, analysis of alternatives, acquisition process, and software engineering--are presented below. The last section of this chapter will relate these specific practices to the five basic objectives.

Requirements Definition

One of the most important activities during the acquisition/development life cycle phase is defining and documenting the user's functional, data, and operational requirements. During requirements definition, the general nature, scope, and objectives of the acquisition/development project should be clearly stated and documented; the project team members should be identified and user interviews should be conducted; existing and new information needs in user operations, functions, or work processes should be defined and analyzed; and a requirements document should be prepared and subjected to management review and approval. Requirements definition primarily relates to the "ensure system effectiveness" objective and heavily involves the user community.

Analysis of Alternatives

During this sub-phase of the acquisition/development life cycle, alternative approaches for economically and efficiently meeting user requirements should be identified and analyzed. A technological feasibility study should be prepared for each alternative and should address key issues, including hardware, software, and communications needs and availability; security and response time constraints; and any legal or regulatory considerations relevant to the technology, such as telecommunications issues. In some cases, an operational feasibility study is needed to assess how the new information system will fit into the agency's current hardware, software, and communications environment. An analysis of project costs and benefits should also be developed to evaluate the economic feasibility of each alternative. Once management reviews these studies and approves an alternative, a master project plan should be prepared to guide the acquisition/development effort.

Acquisition Process

Whether purchasing hardware/software off the shelf or contracting for hardware/software development services, an agency should follow an acceptable acquisition strategy and procurement cycle. The compliance objective is particularly important here since laws, regulations, and standards typically prescribe the steps and activities that should be performed. For example, the Federal Information Resources Management Regulation (FIRMR) requires agencies to select an acquisition

strategy commensurate with project cost, risk, and urgency of need. The FIRMR also describes procurement and contracting rules that apply across the government to certain ADP and telecommunications resource acquisitions. Other relevant laws, regulations, and standards that should be considered in evaluating acquisition projects are listed in the appendix.

Software Engineering

Software engineering is simply defined as a method of building information systems. It includes the key life cycle activities of design and development, controls and back-up, testing and conversion, and quality assurance. In designing and developing software, for example, input, output, file, and processing specifications should be established. Controls and back-up to promote data integrity and safeguard assets should be built into the system design, as well as documentation suitable for use as audit trails. Other software engineering activities include establishing programming objectives and responsibilities, preparing manuals, developing program and system testing standards, and setting system validation and acceptance criteria. Throughout these software engineering activities, the agency's quality assurance group should monitor and assess compliance with standards and procedures, the quality of system design, the adequacy of system program testing, and the completeness of system documentation.

Environmental and Specific Practices Help Achieve the Five Basic Objectives

The preceding sections provided some background information on environmental and specific practices that are important to achieving the five basic objectives during system acquisition/development. This section describes how each objective applies to an acquisition/development project and lists some detailed practices that can help agencies achieve the objectives.

Ensuring System Effectiveness

To be effective, an information system that is being acquired/developed should contribute to achieving the agency's mission, goals, and objectives and to meeting user functional, data, and operational requirements. A formal life cycle process is an important management tool for meeting this objective. While the phases and activities will vary by agency, the process should include heavy user involvement.

In reviewing effectiveness, auditors should identify and evaluate the acquisition/development life cycle process employed by the agency. Using the environmental and specific practices discussed here as a guide, auditors should also consider the

degree of user participation and whether the system being acquired/developed is likely to meet strategic mission requirements and user needs. Some key agency practices for achieving the system effectiveness objective follow.

- The agency has documented its mission, goals, and objectives.
- The agency head has assigned responsibility and established accountability for ADP planning.
- A formal structure or group (e.g., steering committee) involving high-level representatives from every major organizational unit--user department(s), operations, system design and development, security, ADP management, and internal audit (in an advisory capacity)--prepares a long-range ADP plan consistent with agency mission and goals.
- Executive managers assist the agency head in managing information system acquisition/development efforts organization-wide by establishing ADP policies, issuing directives, and approving long-range plans.
- A long-range ADP plan is used to produce short-range plans detailing each acquisition/development project for the upcoming year and its relationship to the agency's mission, goals, and objectives.
- ADP personnel assigned to the project team are adequately qualified to perform their functional responsibilities and are periodically appraised on their performance.
- The agency uses a formal approach to acquire/develop information systems, and involves users in all phases of the approach.
- Users prepare and submit formal requests for new systems.
- User functional, data, and operational requirements are clearly defined, documented, and used in developing the conceptual and detailed design of the system.
- Users review the acquisition project at significant milestones (e.g., completion of detailed design specifications) to verify that all requirements are being met and that resource expenditures should continue.

- Users are involved in preparing test data.
- The system is subject to acceptance testing to ensure that it (1) performs according to the functional and detailed performance specifications and (2) meets user needs and objectives.

Promoting Economy and Efficiency

The acquisition/development process should result in an information system that meets user requirements by using an optimum, least-cost mix of resources. Costs and their corresponding benefits are important considerations in all phases of the acquisition/development process. For example, in evaluating alternative approaches to a software development effort, cost-benefit analyses should be prepared to assist management in selecting the optimum, least-cost alternative. Efficiency, in terms of the resources needed to effectively operate the resultant system, is also an important consideration throughout the acquisition/development process.

In evaluating system economy and efficiency during acquisition/development, auditors should review agency policies and procedures for performing cost-benefit analyses, as well as the actual cost-benefit analysis justifying the acquisition. Auditors should also consider whether the agency's acquisition/development process helps ensure that operational efficiency is built into the system during design and development. The following practices assist agencies in acquiring economical and efficient information systems.

- Agency policies and procedures require cost-benefit analyses of alternative approaches for meeting user needs and provide an appropriate methodology for identifying costs and quantifying benefits.
- The cost-benefit analysis indicates that the selected approach will produce the desired level of benefits in the most economical manner.
- Project management techniques ensure that actual costs are accumulated, reported, and monitored throughout the acquisition process.

- System design incorporates features (e.g., effective forms/terminal design) to optimize performance of the system's manual and automated functions.
 - Performance requirements (e.g., expected data volumes and response times) are established to measure system performance once the system becomes operational.
-

Protecting Data Integrity

To ensure that the planned information system will produce accurate, complete, and reliable data, certain practices should be executed during the acquisition/development process. In the design and development phase, for example, internal ADP auditors should help ensure that adequate audit trails are built into the system design so that transactions can be traced between the processes of origination, input, communications, processing, storage, and output. Additional practices that help agencies protect data integrity in a system being acquired/developed are listed below.

- Key functions performed during the acquisition/development process (e.g., system analysis, application programming, and system programming) are adequately separated.
- The detailed system design, based on the user's output, input, and processing requirements, provides users with the capability to ensure that data are complete, accurate, and authorized.
- Source documents are designed to facilitate accurate information gathering and entry.
- If input data will be introduced on-line, the screen format is designed to promote accuracy and provide edit routines to reduce errors.
- Appropriate hardware controls are built into the peripheral equipment to ensure accurate data transmission within the system, and into the central processing unit to ensure that only valid operations are performed.
- System software contains built-in, error-checking features.
- Testing is performed to evaluate the integrity of the new system with any interfacing system.

- Procedures ensure that no data are lost or erroneously changed in implementing the new system.
-

Safeguarding Information Resources

Protecting resources from waste, loss, unauthorized use, and fraud is the primary intent of this objective. To achieve this goal, an agency should institute practices to ensure that appropriate security measures are designed into the system and that information resources--hardware, software, data, and people--are adequately protected. For the most part, the agency's practices to safeguard information resources, which include separation of duties, supervision of ADP personnel, and documentation of the acquisition/development process, are environmental. Supplemental to these practices are the more acquisition-specific practices listed below.

- User requirements are reviewed to determine the sensitivity of the potential application and the general nature of security needs.
 - The appropriate levels of security are taken into account in defining input and file requirements, procuring hardware, and planning for site modifications.
 - Any vulnerabilities identified during system design and development are reported to management for action.
 - Appropriate protection measures, such as file "lockouts" or passwords, are designed into the system to protect privacy and prevent unauthorized access to sensitive data.
 - Access to the documentation resulting from the acquisition process is restricted to authorized personnel.
 - The system's security features are fully tested, including the system's response to abnormal or unusual circumstances.
-

Complying With Laws and Regulations

In acquiring/developing an information system, an agency should comply with certain laws, regulations, and standards. Auditors are responsible for identifying applicable legislation and guidance and evaluating agency compliance. They should also be alert for other directives and guidance that may affect the acquisition/development project under review, and take note of the agency's internal policies and procedures for implementing the applicable laws and regulations.

**Chapter 3
System Acquisition/Development--
Practices to Meet the Five Basic
Objectives**

The major laws, regulations, and standards relevant to information systems are listed in the appendix, along with a matrix showing which criteria are particularly important to the acquisition/development phase. To assist auditors in evaluating agency compliance, the matrix also shows the primary relationship between these laws, regulations, and standards, and the four other basic objectives.

System Operation/Maintenance-- Practices to Meet the Five Basic Objectives

To meet each of the five basic objectives, agencies should perform certain practices in operating and maintaining their information systems. During system operation/maintenance, environmental and specific practices help agencies

- meet user functional and data requirements;
- use the optimal, least-cost mix of resources to support the agency mission and meet user needs;
- ensure that information is originated, entered, communicated, processed, stored, and reported so that it is accurate, complete, and reliable;
- protect information resources from waste, loss, unauthorized use, and fraud; and
- conform with applicable laws, regulations, and guidance.

This chapter briefly describes key environmental practices applicable to the operation/maintenance life cycle phase, summarizes specific operation/maintenance practices, and relates some of these practices to each of the five basic objectives.

Environmental Practices Help Agencies Achieve the Five Basic Objectives

Environmental practices for operating and maintaining information systems contribute substantially to an agency's achieving the five basic objectives. The practices summarized in this section fall into four broad categories--data center operations, capacity management, telecommunications management, and data center security. Most of the practices in these categories are procedural and relate to operating and maintaining information resources in a computer service center (or data center).

Data Center Operations

Data center operations encompass those practices related to the daily running and maintenance of information systems. For example, effective scheduling of work and preventive maintenance/malfunction reporting have a key role in promoting the efficient flow of data through the center. In addition, the accuracy and completeness of agency information can depend heavily on the policies and procedures followed in the data center.

Input/output scheduling and control

Input/output scheduling and control, which involves continuous tracking of work submitted to and released from the data center, promotes efficient use of computer facilities and helps the agency meet users' information needs. Within the center, a control group should be established to monitor the accuracy and completeness of data received and distributed, schedule computer usage, respond to users' inquiries about the status of work in process or the quality of work performed, and contribute to separation of duties between the computer operators and the system users.

When remote on-line terminals directly link the users to the data center, the computer itself will schedule the work by grouping different jobs for processing. Having a control group oversee these operations can help maintain the integrity of the application.

Preventive maintenance and malfunction reporting

Maintenance of computer systems in the data center generally falls into two categories--preventive maintenance and malfunction repair. Preventive maintenance occurs regularly and includes scheduled inspections and replacement of machine components. System malfunctions occur when a hardware unit malfunctions or the operating system fails and must be modified. Outside vendors are generally responsible for performing both categories of maintenance.

Agencies should develop and follow formal procedures for tracking preventive maintenance and reporting hardware or operating system malfunctions. These reports can provide useful information on the amount of time associated with preventive maintenance and system malfunctions; the level and adequacy of vendor service provided; and the rate of failure, as well as the associated downtime, incurred by the computer system. Operations management should periodically review these reports and use this information to optimize total maintenance costs and system performance.

Capacity Management

Capacity management, which involves managing a system's capability to receive, process, and generate data, encompasses two key areas--resource planning and job accounting/billing. Planning is necessary to ensure that information resources--hardware, software, data, and people--are adequate to provide continuity in processing current applications and to develop new applications as the agency's data processing needs grow. To properly plan for computer capacity, management should have a thorough knowledge of internal agency requirements and an ability to predict the changes in processing workload that could result from internal or external forces. Management must then be able to translate the anticipated needs into resource configurations that are practical, economical, and efficient.

Data processing management should also establish user billing/charge-out policies to encourage fair treatment of user departments and proper usage of information resources in the data center. These policies should define the services chargeable to the user; set up a job accounting system that equitably distributes costs to the system users; and establish billing/charge-out procedures that include provisions for issuing periodic statements to user departments and handling any billing disputes. In addition, management can institute a rate structure that encourages--through options such as lower rates for off-peak service or a sliding scale for varying turnaround requirements--economical and efficient use of information resources.

Telecommunications Management

When an information system relies on a communications network to transmit data between locations, the network should have the capability to safeguard assets, protect data integrity, and allow the information system to meet users' needs economically and efficiently. Evaluating how well the network achieves these objectives is a complex and difficult task involving many variables (for example, network throughput, response time, availability, and reliability). In general, auditors should consider how the network detects and corrects communications errors resulting from hardware/software malfunctions; whether the network relies on public or private lines; how the network is configured around terminals and host computers; and how information on the lines is protected from unauthorized use.

Data Center Security

Data center security procedures help agencies safeguard their information resources against waste, loss, unauthorized use, and fraud. These procedures should focus on

- physically limiting access to the data center to minimize risks;
- establishing "media library controls" to ensure that (1) computer media and documentation are securely stored, (2) access to these resources is limited to authorized personnel, and (3) the media are properly inventoried and circulated; and
- developing a disaster recovery plan to prevent environmental hazards from disrupting data center operations and to provide appropriate back-up if the preventive measures fail.

Developing and implementing these procedures can help data processing management achieve the "safeguard information resources" objective and help protect the integrity of the data processed.

A risk analysis can help data processing management make knowledgeable decisions about environmental hazards and the degree of security required in the data center. While OMB Circular A-130 requires agencies to conduct periodic risk analyses of their information systems at least once every 5 years, it does not specify what activities should be included in these analyses. A risk analysis can range from a simple, qualitative assessment for a small microcomputer system to an in-depth, quantitative examination for a major distributed system. In general, a risk analysis involves identifying the threats or vulnerabilities that a system faces, determining the likelihood of these threats occurring, identifying what resources would be lost and how these losses could be prevented, and balancing the cost of preventive measures against the size and likelihood of losses if the system were not protected.

Specific Practices Focus on Individual Application Systems

Application-specific practices complement environmental practices in ensuring that information systems achieve the five basic objectives. While environmental practices relate to the *whole set* of application systems, specific practices relate to *individual* application systems and focus on the data that flow through the system. The main category of application-specific

practices--the application control framework--is briefly discussed below. The last section of this chapter will relate specific practices from this category to the five basic objectives.

Application Control Framework

An effective application control framework is particularly important in protecting data integrity and safeguarding information resources. All application systems rely on certain processes--data origination, input, communications, processing, storage, and output--to perform their functions. However, the operational mode used to execute these processes can differ with each application, ranging from simple batch systems to on-line, real time operations. This variety of processing modes affects the complexity of the application system under review, as well as the specific practices applied to the system.

In evaluating application-specific controls, auditors need to be familiar with the basic application processes and the operational mode of the system under review. A brief description of the basic application processes follows; the key practices supporting each of these processes are listed later in this chapter, as they relate to the five basic objectives. While a discussion of the many operational modes is beyond the scope of this guide, both batch and on-line practices are presented where possible.

Data origination

Data origination practices are necessary to ensure the accuracy, completeness, and reliability of information before it is entered into the application system. These practices fall into five key areas:

- Data capture, which involves the accurate and timely recording of data.
- Authorization, which includes practices to make sure data are properly authorized and approved.
- Input preparation, which readies the data for further processing.
- Error handling, which ensures that data errors detected at this point are corrected in a timely manner.

- **Retention, which involves properly retaining and backing up data and available source documents so that lost or destroyed information can be recreated.**

While many of the practices in this category are traditionally done manually, agencies are using the computer more and more to verify that the data origination process results in accurate, complete, and authorized information before further processing takes place. The effectiveness of any application system is highly dependent on the quality of source data; consequently, agencies should establish these practices as close to the point of data origin as possible.

Data input

Data input practices are used to ensure the accuracy and completeness of data during conversion into machine readable format and entry into the application system. This process includes practices up to the point where data enter the communications link or, in the absence of communications, to the point of entry into the application program for further processing.

Data input practices focus on three areas--data entry, data validation and editing, and data input error handling. They include both manual and automated practices, depending on the processing mode used. In an on-line system, for example, hardware and software features automatically apply front-end validation and editing routines before transmitting the data to the data center. A batch system, on the other hand, relies more heavily on manual activities, such as verification of control totals and use of logs to account for all batches.

Data communications

Data communications practices are primarily concerned with preserving the integrity of data as they pass from message input devices, through communications lines, to message reception devices. Message input practices help ensure that terminals in use are, in fact, authorized for use and that all messages sent through terminals are identifiable. During message transmission, communications practices focus on checking messages as they flow over the lines and on certain physical characteristics of the lines themselves. Message reception practices relate to the hardware and software in the computer system and how they receive and account for all messages in

the system. With the growing trend to use data communications as an integral part of an application system, auditors are having to expand their communications knowledge and expertise.

Computer processing

Computer processing practices are necessary to ensure that complete and accurate information is processed between data input and output. These practices begin with entry of data into the central processing unit and end with either data storage and/or output reporting. The key objective in this category is to properly use the appropriate programs and files so that updates are accurately performed and the resulting output is correct.

Data storage

Data storage and retrieval practices involve preparing a file for use by the application system. These practices also help ensure that complete and accurate data are maintained during periods when the data are not being used by the application system. Since this process involves a high degree of human intervention by the media librarian and computer operation personnel, file handling practices should be accurately performed and monitored. Data storage and retrieval practices should safeguard data files and programs; promote efficient use of files and programs; and make sure that errors are detected, corrected, and reprocessed.

Where data base systems are used, proper data base administration provides a focal point for defining and controlling all elements of the system, including the protection of data. A data base is a collection of interrelated data that is stored together to serve multiple users and application programs. The data base administrator is the manager responsible for coordinating the design and use of the data base and the data base management system, educating and training users about the system, and controlling user interfaces and access to the data.

Output

Output practices ensure the integrity of data is maintained, from the conclusion of computer processing until delivery of output (through either hard-copy documents or terminal display) to the user. Since users depend on timely and accurate delivery of output data to perform their work, these practices are an

important interface between the data processing staff and the user departments. In most cases, if the application system has strong data origination, input, and processing practices, the output will be accurate and reliable. Output practices emphasize balancing and reconciliation, output distribution, and records retention.

Environmental and Specific Practices Help Achieve the Five Basic Objectives

The preceding sections provided insights into the environmental and application-specific practices that are important to achieving the five basic objectives during system operation and maintenance. This section describes each of the five objectives in terms of the operational life cycle phase and lists some detailed practices that can help agencies achieve the objectives.

Ensuring System Effectiveness

To be effective, an information system should operate as intended and provide users with the information they need, in the proper format. It should also meet users' needs for timeliness, accuracy, completeness, and reliability. The following practices can guide auditors in determining if an operational system achieves this objective.

- User functional and data requirements for the system have been adequately identified and documented.
- The system is properly maintained to help ensure continued responsiveness to the users.
- The system's ability to meet user needs was preserved during any change or modification activities.
- User requirements are periodically re-evaluated to determine if system changes are needed.
- Procedures for requesting changes to the system are documented and followed by the users.

Promoting Economy and Efficiency

Systems should be operated and maintained so that user functional and data requirements are met using the optimum, least-cost mix of information resources. Economy and efficiency depends in large part on the environment in which the system operates. In managing hardware and software resources, for example, agencies need to collect and analyze data on system capacity and performance. This data should be used to plan current and future resource needs and to "tune" the existing

system to improve performance. Economy and efficiency gains can also be achieved by giving careful attention to how the overall system is operated and maintained. Finally, where data communications is an important part of the application, proper network management will contribute to an economical and efficient environment.

To provide the type of environment highlighted above, agencies should do the following:

- Develop and implement formal resource planning methods for projecting hardware, software, data, and personnel needs, and mechanisms for analyzing variances between actual and planned goals.
- Use computer performance management tools (e.g., hardware and software monitors) to collect and analyze data on system performance.
- Perform capacity management to analyze the loading, utilization, and response of the system and to control the flow of current and future work through the system.
- Institute an input/output scheduling and control function to schedule, monitor, and control the day-to-day information processing workflow.
- Design and implement a job billing and charge-out system that accounts for and charges operational costs to users, creating an incentive to use the least-cost mix of resources.
- Conduct and track preventive maintenance on computer hardware to keep it in good working order.
- Develop and follow formal procedures for reporting, documenting, and resolving system malfunctions.
- Direct operations management to periodically review maintenance and malfunction records and use this information to optimize total maintenance costs and system performance.
- Monitor network operations to detect, document, and resolve problems that inhibit efficient functioning.

Protecting Data Integrity

Environmental and specific practices have a key role in ensuring data accuracy, completeness, and reliability. The environmental practices critical to achieving the data integrity objective include documented operating policies and procedures, separation of duties, and media library controls. The application-specific practices also play a significant role in achieving this objective.

Key environmental practices for achieving the protect data integrity objective are listed below, followed by application-specific practices for data origination and input, communications, processing, storage, and output.

- Operating policies and procedures are adequately documented, communicated, and followed by employees.
- Key operations functions--production scheduling, equipment operation, application/system programming, data origination, data entry, and data base management--are performed by different groups or individuals, and this separation of duties is enforced.
- An audit trail exists that allows data to be traced forward to the final output and backward to the point of origin.
- Specific authorization is required for all types of transactions.

Data origination and input practices

- Source documents are designed to minimize errors and omissions and to ensure data uniformity.
- Data submitted for conversion and entry are properly accounted for and monitored.
- System features and/or procedures promote validation, editing, and control of transactions as close to their point of origin as possible.
- Erroneous transactions rejected during the input process are corrected and re-entered in a timely manner.
- Overriding or bypassing edit and validation routines is restricted to supervisors and permitted on a limited basis.

Data communications practices

- Telecommunications hardware and software have built-in controls to detect and report errors in data transmissions.
- Both incoming and outgoing messages are checked for valid addresses.
- Appropriate hardware and software features exist to make sure all messages that are sent are also received.

Computer processing practices

- Application programs have provisions to prevent unauthorized updates and deletions.
- Application programs perform relationship editing and validation routines to ensure that incorrect data are rejected before updating the master file.
- Data rejected by the application program are properly identified, controlled, corrected, and reprocessed.

Data storage and retrieval practices

- File handling controls (e.g., internal file label checks) ensure proper storage and retrieval of data files.
- System features (e.g., special control information on internal file labels) help to ensure that the contents of data files are not overwritten or erased before the end of their useful life.
- A feature in the file accessing routine prohibits two programs from simultaneously updating the same application record.
- A data dictionary is used to accurately and completely define data contained in the data base.

Output practices

- Reports or other output are promptly distributed to authorized users.
- Procedures and/or system features exist to identify and control errors contained in output.

- Output totals are properly reconciled to make sure the output is accurate and complete.
-

Safeguarding Information Resources

A variety of environmental and specific practices protects a system's information resources--its hardware, software, data, and people--from waste, loss, unauthorized use, and fraud. These practices are applied in several ways. For example, physical protection is used to prevent unauthorized access to agency facilities where hardware, software, and data are maintained and stored. Logical protection, which involves internal system controls, is used to prevent unauthorized access to the agency's system software, application programs, and data bases. Finally, back-up systems and procedures prevent loss of service during unanticipated interruptions and disasters. Key environmental practices are listed below.

- Physical barriers (e.g., locked doors, solid walls) and automated security devices (e.g., keys, badges) restrict access to computer facilities.
- Facilities and files are physically protected from environmental hazards, including fire, water damage, and power failures.
- Terminals are located in areas that reduce the risk of unauthorized viewing of data.
- Access to source documents and critical forms (e.g., negotiable instruments, identification cards) is restricted to authorized personnel.
- Data files are under the strict control of a media librarian at all times.
- Application systems documentation is physically secure and access is restricted to authorized staff.
- Access to on-line data is restricted by requiring proper identification and passwords.
- Use of system software that allows the bypassing of normal controls is either prohibited or strictly controlled.

- Documented procedures are followed for the back up of critical data files and programs and for the recovery of information system services in the event of an unanticipated disaster or interruption.
- A back-up plan, which provides for alternate computer facilities in the event of a disaster, is periodically tested and updated.
- Management regularly reviews the propriety of terminal authority levels and periodically changes all passwords. Passwords are also changed when an employee changes jobs or leaves the organization, and when purported or real security violations occur.
- Employees with access to sensitive data receive security clearances that are periodically updated.
- Agencies conduct appropriate risk analyses of their data processing operations according to relevant guidance and procedures.

Complying with Laws and Regulations

An agency should operate and maintain its information systems according to certain laws, regulations, and standards. Auditors are responsible for identifying applicable legislation and guidance and evaluating agency compliance. The major laws, regulations, and standards relevant to information systems are listed in the appendix . A matrix showing which of these criteria are applicable to the operation/maintenance life cycle phase, as well as the primary relationship between these laws, regulations, and standards and the four basic objectives discussed earlier, is also included in the appendix.

Crosswalk to Additional Guidance

Auditing the acquisition/development and operation/maintenance of an information system involves collecting and evaluating information to determine if a system meets or will meet the five basic objectives. To aid in this process, the guide has briefly summarized some of the broad categories of environmental and specific practices that are critical in acquiring and operating information systems. The guide further highlights how some of the detailed practices in these categories relate to the five basic objectives during each life cycle phase. Taken together, this approach provides a logical framework for evaluating agency acquisition and use of information systems.

To assist staff in using this guide, the following sections describe (1) how the guide relates to GAO's job planning and management process and (2) what additional GAO guidance on auditing information systems is available. These two sections should serve as a useful supplement to the conceptual framework presented in the guide.

Linkage Between the Guide and GAO's Job Management Framework

The guide promotes audit flexibility and coordinates well with GAO's job planning and management process, which is fully described in GAO's internal Project Manual. While the guide provides an "objectives-based" framework for evaluating the acquisition and use of information systems, the GAO job planning process sets up a "project-based" framework for managing individual assignment phases and decisions.

The GAO job management framework provides a flexible, results-oriented approach to decisionmaking. It generally consists of five phases, including the

- proposal phase, which justifies studying a particular area;
- scoping phase, which determines the approach that will be taken to a project;
- planning phase, which spells out how the project will be carried out and assigns responsibilities to each staff member;
- implementation phase, which involves performing audit work and redirecting the assignment as necessary; and
- evaluation and follow-up phase, which formally evaluates the assignment results and staff performance.

Throughout each phase, key decision components--such as issue and approach, customer, and timing--may be used to manage an assignment and determine whether or not it should proceed as planned.

The guide, with its broad coverage of the practices important to system acquisition and operation, should prove extremely useful during the proposal, scoping, planning, and early implementation phases. The five basic objectives defined in the guide provide a consistent foundation for building individual assignment objectives and approaches. By highlighting the most significant practices that should be present in the agency environment, the guide should help in identifying potential areas for review and in planning work.

Linkage Between the Guide and Available Criteria

Since the intent of this guide is to provide a conceptual framework for evaluating agency acquisition and use of information systems, it contains high-level discussions of the life cycle process, the five basic objectives, key categories of agency practices, and the relationship between these practices and the five basic objectives. It does not outline the audit steps needed to identify the controls or practices that exist at the agency, list evidence to be collected, or describe tests to verify that the the controls or practices in place actually function as intended.

To complement the conceptual framework established in the guide, auditors who are evaluating system acquisition/development efforts should consult the appendix and review applicable laws, regulations, and standards. Auditors evaluating system operation/maintenance should also review the appendix for applicable criteria, and they should use appropriate sections of GAO's audit guide entitled, Evaluating Internal Controls in Computer-Based Systems (June 1981), which contains more detailed audit steps and evaluation criteria.

The Compliance Objective-- Key Laws, Regulations, and Standards

Laws, Regulations, and Directives

Laws

- Accounting and Auditing Act of 1950 (64 STAT. 834) requires the head of each executive agency to establish and maintain adequate systems of accounting and internal control.
- Brooks Act of 1965, Public Law 89-306 (40 U.S.C. 759), is the primary law governing federal acquisition and management of ADP equipment.
- Competition in Contracting Act of 1984, Public Law 98-369 (40 U.S.C. 759(h)), requires full and open competition as the primary method of procurement, except under specific, well-defined circumstances. It also authorizes the General Services Administration's Board of Contract Appeals to decide protests involving ADP procurement conducted according to the Brooks Act, Public Law 89-306.
- Federal Managers' Financial Integrity Act of 1982 (FMFIA), Public Law 97-255 (31 U.S.C. 3512), requires executive agencies to perform ongoing evaluations and report annually on the adequacy of their systems of internal accounting and administrative control.
- Federal Property and Administrative Services Act of 1949, as amended (63 STAT. 377), provides basic procurement and management authority, including the procurement and management of telecommunications.
- Federal Records Management Amendments of 1976, Public Law 94-575 (44 U.S.C. 2901), require the establishment of standards and procedures to ensure efficient and effective federal records management practices.
- Paperwork Reduction Act of 1980, Public Law 96-511 (44 U.S.C. 3501), sets up mechanisms to reduce federal paperwork and to improve federal information policy-making by ensuring, among other things, that ADP and telecommunications technology is acquired and used effectively and efficiently.
- Privacy Act of 1974, Public Law 93-579 (5 U.S.C. 552a), establishes individuals' right to review records that

federal agencies maintain about them and establishes a code of fair recordkeeping practices, including a standard of accuracy, limitations on disclosure of records, and safeguards for records.

Regulations

- Federal Information Resources Management Regulation (FIRMR) (41 CFR Ch. 201) is the primary regulation governing federal agencies' management, acquisition, and use of certain ADP and telecommunications resources. The FIRMR is to be used in conjunction with the general procurement and contracting regulations contained in the Federal Acquisition Regulation.
- Federal Acquisition Regulation is the primary regulation for use by all federal executive agencies in their acquisition of supplies and services with appropriated funds.

Directives

- Department of Defense (DOD) Directive No. 7920.1, "Life Cycle Management of Automated Information Systems," October 17, 1978, establishes joint technical and functional policy governing the life cycle management and control of automated information systems.
- DOD Directive No. 7920.2, "Major Automated Information Systems Approval Process," October 20, 1978, supplements the provisions of DOD Directive 7920.1 by establishing the review and decision process and procedures for automated information systems.
- National Security Decision Directive (NSDD) 145, "National Policy on Telecommunications and Automated Information Systems Security," issued by the White House, September 17, 1984, sets the National Security Agency as the focal point for both military and civilian information security, including cryptography, telecommunications systems security, and automated systems security.

**Appendix
The Compliance Objective--
Key Laws, Regulations, and Standards**

**Table I.1: Key Laws, Regulations, and Directives--
Relationship to the Other Information System Objectives**

Objectives Criteria		Ensure System Effectiveness	Promote System E and E	Protect Data Integrity	Safeguard Information Resources
L A W S	Accounting and Auditing Act of 1950			O	O
	Brooks Act of 1965	A	A		
	Competition in Contracting Act of 1984		A		
	FMFIA			O	O
	Federal Property and Administrative Services Act of 1949	A	A		
	Federal Records Mgmt. Amendments of 1976	O	O	O	O
	Paperwork Reduction Act of 1980	A, O	A, O		
	Privacy Act of 1974			O	A, O
R E G S	FIRMR	A, O	A, O		A, O
	Federal Acquisition Regulation	A	A		
D I R	DOD Directive 7920.1	A, O	A, O		
	DOD Directive 7920.2	A, O	A, O		
	NSDD - 145				A, O

Legend: "E and E" means economy and efficiency.
 "A" indicates relevance to the acquisition/development life cycle phase.
 "O" indicates relevance to the operation/maintenance life cycle phase.

OMB Circulars

- Circular No. A-11, Preparation and Submission of Budget Estimates (Transmittal Memorandum No. 54), revised July 19, 1983, provides detailed guidance on preparing budget estimates. Section 43 addresses data processing and telecommunications systems. Section 24 requires budget justification for data processing and telecommunications equipment, based on programmatic need.
- Circular No. A-71, Responsibilities for the Administration and Management of Automatic Data Processing Activities, March 6, 1965, specifies responsibilities for acquiring and managing ADP equipment and activities. (Superseded by Circular No. A-130, effective December 12, 1985.)
- Circular No. A-71 (Transmittal Memorandum No. 1), Security of Federal Automated Information Systems, July 27, 1978, provides guidance on the security of federal automated information systems. (Superseded by Circular No. A-130, effective December 12, 1985.)
- Circular No. A-76, Performance of Commercial Activities, revised August 4, 1983, establishes the policy that private enterprise is the preferred source of supply for commercial or industrial goods and services (including ADP), unless it costs significantly more or is not in the government's best interest.
- Circular No. A-108, Responsibilities for the Maintenance of Records About Individuals by Federal Agencies, July 1, 1975, and Transmittal Memorandum Nos. 1-4, prescribe policies and procedures for implementing the Privacy Act. Transmittal Memorandum No. 5 discusses telecommunications responsibilities regarding the Act. (Superseded by Circular No. A-130, effective December 12, 1985.)
- Circular No. A-109, Major System Acquisitions, April 5, 1976, describes the policies and procedures for federal acquisitions of major systems.
- Circular No. A-121, Cost Accounting, Cost Recovery, and Interagency Sharing of Data Processing Facilities, September 16, 1980, establishes policies to promote effective and efficient management and use of certain data processing facilities. (Superseded by Circular No. A-130, effective December 12, 1985.)

-
- Circular No. A-123, Internal Control Systems, August 16, 1983, provides policies and procedures on internal controls to be followed by executive departments and agencies.
 - Circular No. A-130, Management of Federal Information Resources, December 12, 1985, provides a general policy framework for management of federal information resources. The Circular implements provisions of the Paperwork Reduction Act of 1980, as well as other statutes and policies concerning information technology, privacy, and maintenance of federal records. It supersedes OMB Circular Nos. A-71, A-90, A-108, and A-121, as well as all Transmittal Memorandums to those Circulars.

GAO Standards

- Policy and Procedures Manual for Guidance of Federal Agencies, Title 2-Accounting, revised November 14, 1984, prescribes the overall accounting principles for executive agencies. Appendix II, "Internal Control Standards," restates GAO Accounting Series, "Standards for Internal Controls in the Federal Government," issued in June 1983.
- Illustrative Accounting Procedures for Federal Agencies, Guidelines for Accounting for Automatic Data Processing Costs, (Pamphlet No. 4), 1978, supplements Title 2 (see above) by providing guidance on accounting for data processing costs.
- Standards for Audit of Governmental Organizations, Programs, Activities, and Functions ("Yellow Book," 1981 Revision) contains standards that auditors must follow in reviewing government operations.

**Appendix
The Compliance Objective--
Key Laws, Regulations, and Standards**

**Table I.2: Key OMB Circulars and GAO Standards --
Relationship to the Other Information System Objectives**

Objectives		Ensure System Effectiveness	Promote System E and E	Protect Data Integrity	Safeguard Information Resources
Criteria					
O M B C I R C U L A R S	Circular No. A-11	A	A		
	Circular No. A-71	A, O	A, O		
	Circular No. A-71, Transmittal No. 1				O
	Circular No. A-76		A		
	Circular No. A-108			O	O
	Circular No. A-109	A	A		A
	Circular No. A-121		A, O		
	Circular No. A-123	O	O	O	O
	Circular No. A-130	A, O	A, O	O	O
G A O S T A N D A R D S	Policy and Procedures Manual for Guidance of Federal Agencies, Title 2, Accounting-- App. II, Internal Control Standards	O	O	O	O
	Guidelines for Accounting for ADP Costs, Pamphlet No. 4	A, O	A, O	A, O	
	Standards for Audit of Governmental Organizations, Programs, Activities, and Functions	A, O	A, O	A, O	A, O

Legend: "E and E" means economy and efficiency.
 "A" indicates relevance to the acquisition/development life cycle phase.
 "O" indicates relevance to the operation/maintenance life cycle phase.

Federal Information Processing Standards Publications (FIPS PUBs)

- FIPS PUB 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, June 1974, provides guidelines for federal organizations to use in structuring physical security programs for their ADP facilities. It can be used as a checklist for planning and evaluating the security of computer systems.
- FIPS PUB 38, Guidelines for Documentation of Computer Programs and Automated Data Systems, February 15, 1976, provides basic guidance in preparing documentation used in developing computer software and serves as a checklist for planning and evaluating software documentation practices.
- FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974, May 30, 1975, provides guidance in selecting technical and related procedural methods to protect personal data in automated information systems.
- FIPS PUB 42-1, Guidelines for Benchmarking ADP Systems in the Competitive Procurement Environment, May 15, 1977, recommends good practices for federal agencies to use in planning, organizing, and conducting benchmark demonstrations for competitive computer procurements.
- FIPS PUB 49, Guideline on Computer Performance Management: An Introduction, May 1, 1977, details ADP managers' responsibilities in meeting user requirements, managing and planning for ADP resources, and communicating with upper management and computer vendors.
- FIPS PUB 64, Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase, August 1, 1979, provides guidance in determining the content and extent of documentation needed for the initiation phase of the software life cycle, including project requests, feasibility studies, and cost/benefit analyses.
- FIPS PUB 65, Guideline for ADP Risk Analysis, August 1, 1979, presents a technique for conducting a risk analysis of an ADP facility and the related assets.
- FIPS PUB 73, Guidelines for Security of Computer Applications, June 30, 1980, outlines methods and technique

to reduce the security hazards associated with computer applications.

- FIPS PUB 75, Guideline on Constructing Benchmarks for ADP System Acquisitions, September 18, 1980, describes a step-by-step procedure for use in acquiring ADP systems.
- FIPS PUB 76, Guideline for Planning and Using a Data Dictionary System, August 20, 1980, describes the capabilities of and provides guidance for implementing and operating a data dictionary system.
- FIPS PUB 87, Guidelines for ADP Contingency Planning, March 27, 1981, offers guidelines for preparing ADP contingency plans.
- FIPS PUB 88, Guideline on Integrity Assurance and Control in Database Administration, August 14, 1981, provides explicit advice on achieving data base integrity and security control.
- FIPS PUB 101, Guideline for Lifecycle Validation, Verification, and Testing of Computer Software, June 6, 1983, presents an integrated approach to validation, verification, and testing that should be used throughout the software life cycle. Includes a glossary of technical terms.
- FIPS PUB 102, Guideline for Computer Security Certification and Accreditation, September 27, 1983, describes how to establish and carry out a certification and accreditation program for computer security over sensitive applications.
- FIPS PUB 105, Guideline for Software Documentation Management, June 6, 1984, provides advice on managing the planning, development, and production of computer software documentation. It also includes references to relevant standards, guidelines, and literature on software documentation and a glossary of terms.
- FIPS PUB 106, Guideline on Software Maintenance, June 15, 1984, presents information on techniques, procedures, and methodologies to employ throughout the life cycle of a software system to improve the maintainability of that system. It also discusses controlling and improving software maintenance.

- **FIPS PUB 110, Guideline for Choosing a Data Management Approach**, December 11, 1984, outlines guidance for identifying and selecting a data management approach appropriate to organizational requirements.
- **FIPS PUB 112, Password Usage**, May 30, 1985, specifies basic security criteria for two different uses of passwords in an automatic data processing system: (1) personal identity authentication and (2) data access authorization.

**Appendix
The Compliance Objective--
Key Laws, Regulations, and Standards**

**Table I.3: Key FIPS PUBs--
Relationship to the Other Information System Objectives**

Objectives Criteria		Ensure System Effectiveness	Promote System E and E	Protect Data Integrity	Safeguard Information Resources
FIPS PUB L I C A T I O N S	FIPS PUB 31				A, O
	FIPS PUB 38	A, O	A, O	A, O	A, O
	FIPS PUB 41				A, O
	FIPS PUB 42-1	A	A		
	FIPS PUB 49	A, O	O		A
	FIPS PUB 64	A	A	A	A
	FIPS PUB 65				O
	FIPS PUB 73				O
	FIPS PUB 75	A	A		
	FIPS PUB 76			O	
	FIPS PUB 87				O
	FIPS PUB 88			O	O
	FIPS PUB 101	A, O	A, O	A, O	
	FIPS PUB 102				A, O
	FIPS PUB 105	A, O	A, O	A, O	A, O
	FIPS PUB 106	O	O	O	
FIPS PUB 110	O	O	O	O	
FIPS PUB 112			O	O	

Legend: "E and E" means economy and efficiency.
 "A" indicates relevance to the acquisition/development life cycle phase.
 "O" indicates relevance to the operation/maintenance life cycle phase.

Requests for copies of GAO publications should be sent to

U. S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877

Telephone 202-275-6241

The first five copies of each publication are free. Additional copies are \$2.00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.

United States
General Accounting Office
Washington, D.C. 20548

Official Business
Penalty for Private Use \$300

Address Correction Requested

Special Fourth Class Rate Postage & Fees Paid GAO Permit No. G100
