United States General Accounting Office

GAO

Accounting and Information
Management Division

Federal Information System Controls Audit Manual

Volume I - Financial Statement Audits

GAO/AIMD-12.19.6

PREFACE

Federal agencies, the Congress, and the public rely on computer-based information systems to carry out agency programs, manage federal resources, and report program costs and benefits. The methodology outlined in this manual provides guidance to auditors in evaluating internal controls over the integrity, confidentiality, and availability of data maintained in these systems. The manual is primarily designed for evaluations of general and application controls over financial information systems that support agency business operations. However, it could also be used when evaluating the general and application controls over computer-processed data from agency program information systems, as called for in Government Auditing Standards.[1]

We envision that this manual will be used primarily to assist auditors in reviewing internal controls as part of the annual financial statement audits that are now required at all major federal agencies. The manual is designed for information systems auditors and financial auditors who have demonstrated that they have the necessary knowledge, skills, and abilities to perform audit procedures in a computer-based environment, which are discussed in Appendix V. We expect that the manual will serve as a common language between information system auditors and financial auditors so that they can effectively work together as a team, understand the tasks to be accomplished, and achieve common goals.

The manual is a companion to GAO's Financial Audit Manual (FAM) and discusses the control objectives that auditors should consider when assessing computer-related controls, and it provides examples of control techniques commonly used at federal agencies along with suggested audit procedures. For some areas, auditors may need to obtain specialized technical assistance to carry out these procedures. This manual is Volume I of two volumes. We plan Volume II to contain audit practice aids for addressing specific software products, such as access control software and selected computer operating systems.

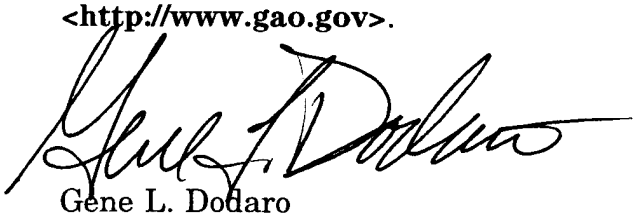
COMMENTS ON THIS GUIDE

Any questions about the applicability of this manual should be directed to the Director of Planning and Reporting, Accounting and Information Management Division, or the Director of Consolidated Audit and Computer Security Issues, who can be reached at (202) 512-9450 and (202) 512-3317, respectively. Major

---

[1]Government Auditing Standards: 1994 Revision (GAO/OCG-94-4), Paragraph 6.62, "Validity and Reliability of Data From Computer-Based Systems."

instructions and the address for submitting comments. We plan to periodically revise sections of this manual based on comments from users and our own experience in applying the manual. An electronic version of this manual is available from GAO's World Wide Web server at the following Internet address: **<http://www.gao.gov>**.



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

January 1999

TABLE OF CONTENTS

[This page is intentionally left blank.]

CHAPTER 1

INTRODUCTION AND GENERAL METHODOLOGY

As computer technology has advanced, federal agencies have become increasingly dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. As a result, the reliability of computerized data and of the systems that process, maintain, and report these data are a major concern to auditors of federal entities. Auditors may need to evaluate the reliability of computer-generated data supporting financial statements or used to analyze specific program costs and outcomes. In addition, auditors may be called on to evaluate the adequacy of controls in systems to help reduce the risk of loss due to errors, fraud, and other illegal acts and disasters or other incidents that cause the systems to be unavailable.

1.1 PURPOSE AND ANTICIPATED USERS OF THE MANUAL

This manual describes the computer-related controls that auditors should consider when assessing the integrity, confidentiality, and availability of computerized data. It is a guide applied by GAO primarily in support of financial statement audits and is available for use by other government auditors. It is not an audit standard. Its purposes are to

- inform financial auditors about computer-related controls and related audit issues so that they can better plan their work and integrate the work of information systems (IS) auditors with other aspects of the financial audit and
- provide guidance to IS auditors on the scope of issues that generally should be considered in any review of computer-related controls over the integrity, confidentiality, and availability of computerized data associated with federal agency systems.

The manual lists specific control techniques and related suggested audit procedures. However, the audit procedures provided are stated at a high level and assume some expertise about the subject to be effectively performed. As a result, more detailed audit steps generally should be developed by the IS auditor based on the specific software and control techniques employed by the auditee after consulting with the financial auditor about audit objectives and significant accounts. Many of the suggested audit procedures start with the word "review." We intend the auditor to do more than simply look at the subject to be reviewed. Rather, we envision a critical evaluation where the auditor uses professional judgment and experience and undertakes the task with a certain level of skepticism, critical thinking, and creativity.

Although IS audit work, especially control testing, is generally performed by an IS auditor, financial auditors with appropriate training, expertise, and supervision may undertake specific tasks in this area of the audit. This is especially appropriate during financial statement audits where the work of financial auditors and IS auditors must be closely coordinated. Throughout this manual, the term "auditor" should generally be interpreted as either (1) an IS auditor or (2) a financial auditor working in consultation with or under the supervision of an IS auditor.

1.2 GENERAL METHODOLOGY

The general methodology that should be used to assess computer-related controls involves evaluating

- general controls at the entity or installation level;
- general controls as they are applied to the application(s) being examined, such as a payroll system or a loan accounting system; and
- application controls, which are the controls over input, processing, and output of data associated with individual applications.

General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. Examples of primary objectives for general controls are to safeguard data, protect computer application programs, prevent system software from unauthorized access, and ensure continued computer operations in case of unexpected interruptions. The effectiveness of general controls is a significant factor in determining the effectiveness of application controls. Without effective general controls, application controls may be rendered ineffective by circumvention or modification. For example, edits designed to preclude users from entering unreasonably large dollar amounts in a payment processing system can be an effective application control. However, this control cannot be relied on if the general controls permit unauthorized program modifications that might allow some payments to be exempt from the edit.

Application controls are directly related to individual computerized applications. They help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. Application controls include (1) programmed control techniques, such as automated edits, and (2) manual follow-up of computer-generated reports, such as reviews of reports identifying rejected or unusual items.

Both general and application controls must be effective to help ensure the reliability, appropriate confidentiality, and availability of critical automated information.

Determining the Nature and Extent of Audit Procedures

The nature and extent of audit procedures required to assess computer-related controls varies depending on the audit objectives and other factors. Factors to consider include the nature and complexity of the entity's information systems, the entity's control environment, and particular accounts and applications that are significant to the financial statements. The information systems auditor and financial auditor should work cooperatively to determine what review work is necessary. When performed as part of a financial statement audit, an assessment of computer-related controls is part of a comprehensive effort to evaluate both the controls over and reliability of reported financial data. The following pages provide an overview of the tasks involved in reviewing computer-related controls for a financial statement audit.

Reviewing Computer-related Controls in Financial Statement Audits

Financial statement audits under the Chief Financial Officers Act of 1990 are intended to play a central role in (1) providing more reliable and useful financial information to decisionmakers and (2) improving the adequacy of internal controls and underlying financial management systems. Computer-related controls are a significant factor in achieving these goals and in the auditor's understanding of the entity's internal control structure. Computer-related controls should be considered during all four phases of the audit: the planning phase, the internal control phase, the testing phase, and the reporting phase. GAO's Financial Audit Manual provides detailed guidance on the four phases of a financial statement audit, as well as overall audit objectives and testing and reporting requirements for such audits. However, most evaluation of computer-related controls will take place in the planning and internal control phase, the results of which will affect the nature, timing, and extent of substantive testing in the testing phase. Audit activities pertaining to computer-related controls during each phase of a financial statement audit are discussed below.

Planning Phase

During the planning phase, the auditor gains an understanding of the entity's computer-related operations and controls and related risks. In view of these risks, the auditor tentatively concludes which controls are likely to be effective. If the controls are likely to be effective and if they are relevant to the audit objectives, the auditor should determine the nature and extent of the audit work needed to confirm his or her tentative conclusions. If the controls are not likely to be effective, the auditor should obtain a sufficient understanding of related control risks to (1) develop appropriate findings and related recommendations for corrective action and (2) determine the nature, timing, and extent of substantive testing that will be needed. Audit planning is discussed further in Chapter 2.

Internal Control Phase

During the internal control phase, auditors obtain detailed information on control policies, procedures, and objectives and perform tests of control activities. The objectives of these tests are to determine if controls are operating effectively.

The auditor first tests entity- or installationwide general controls through a combination of procedures, which include observation, inquiry, and inspection. The auditor may also reperform a control being tested to determine if it was properly applied. If these controls are operating effectively, the auditor should then test and evaluate the effectiveness of general controls for the applications that are significant to the audit.

If general controls are not operating effectively, the application-level controls are generally not tested. Without effective general controls, application controls may be rendered ineffective by circumvention or modification. In such cases, the auditor should develop appropriate findings and consider the nature and extent of risks, since these risks are likely to affect substantive tests. However, if an audit objective is to identify control weaknesses with an application where more employees may have the potential to take advantage of a weakness, an assessment of the application controls may be appropriate. Also, when weaknesses exist mainly in general control areas having a less significant impact on application-level controls and the financial statements, and general controls having a more significant impact are effective, such as access controls, testing of application controls may be warranted.

If general controls are determined to be adequate for the relevant applications, the auditor then proceeds to test the application controls that the financial auditors, with assistance from information systems auditors, have identified as critical to the reliability of the data supporting the financial statements. These controls are generally designed to prevent, detect, and correct errors and irregularities as transactions flow through the financial information systems. The objectives of these controls are specific to the applications they support. However, they generally involve ensuring that

- data prepared for entry are complete, valid, and reliable;
- data are converted to an automated form and entered into the application accurately, completely, and on time;
- data are processed by the application completely and on time, and in accordance with established requirements; and
- output is protected from unauthorized modification or damage and distributed in accordance with prescribed policies.

The auditor evaluates and tests the effectiveness of application controls by observing

the controls in operation, examining related documentation, discussing the controls with pertinent personnel, and reperforming the control being tested.

Testing Phase

The testing phase of a financial audit focuses primarily on substantive tests. These tests generally involve examining source documents that support transactions to determine if they were recorded, processed, and reported properly and completely. An IS auditor may assist financial auditors in identifying and selecting computer-processed transactions for testing, possibly using computer audit software. However, such assistance is not detailed in this version of the manual.

Reporting Phase

During the reporting phase, the financial auditor draws conclusions and reports on the financial statements, management's assertions about internal controls, and compliance with laws and regulations. Regarding internal controls, the GAO auditor expresses an opinion on management's assertions about whether the internal controls in effect at the end of the period are sufficient to meet the following control objectives, insofar as those objectives pertain to preventing or detecting losses, noncompliance, or misstatement that would be material in relation to the financial statements:

- Assets are safeguarded against loss from unauthorized acquisition, use, or disposition.
- Transactions are executed in accordance with budget authority and with laws and regulations tested by the auditor.
- Transactions are properly recorded, processed, and summarized to permit the preparation of financial statements and to maintain accountability for assets.[2]

The combined evaluations of the entity's internal controls form the basis of the auditor's opinion on management's assertions on internal controls. The auditor develops an opinion by concluding as to the effectiveness of controls and comparing this conclusion with management's assertions. In evaluating the audit results and developing the opinion on management's assertions, the financial auditors and the IS auditor should work together so that computer-related control evaluation results are adequately considered and properly reported.

In concluding on the effectiveness of controls, the auditor should determine if any weaknesses identified are significant enough to be reportable conditions and if any of

[2]Expressing this opinion is not currently the practice for non-GAO federal auditors, although audit guidance does indicate that rendering such an opinion may be required in future years.

these reportable conditions represent material weaknesses. (The criteria for determining if weaknesses represent reportable conditions or material weaknesses are discussed in Section 580.36 of GAO's Financial Audit Manual.) Material weaknesses and other reportable conditions should be communicated to the entity head, the Office of Management and Budget, and the Congress in the auditor's report on the annual financial statements. Reportable conditions should be accompanied by suggestions for corrective actions.

The auditor may report weaknesses that do not meet the criteria for reportable conditions in a letter to management or orally to an appropriate level of the entity. The auditor may include suggestions for corrective action for these less significant weaknesses if enough is understood about their cause. (More detailed information on precisely how and where control weaknesses should be reported for annual financial statement audits is presented in Sections 580.48 through 580.52 of GAO's Financial Audit Manual.)

Regardless of where they are reported, computer-related control weaknesses should be described clearly in terms that are understandable to individuals who may have limited expertise regarding information systems issues. In this regard, the report should clearly define technical terms and avoid jargon and acronyms.

The report should discuss each weakness in terms of the related criteria, the condition identified, the cause of the weakness, and the actual or potential impact on the entity and on those who rely on the entity's financial data. This information helps senior management understand the significance of the weakness and develop appropriate corrective actions. For most types of computer-related control weaknesses, this manual includes a discussion of risks and potential negative effects that can be adapted for audit reports. GAO has issued several reports that can be used as models for reporting computer-related weaknesses. These include Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure (GAO/AIMD-98-175, September 23, 1998); Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations (GAO/AIMD-98-145, May 18, 1998); and Federal Family Education Loan Information System: Weak Computer Controls Increase Risk of Unauthorized Access to Sensitive Data (GAO/AIMD-95-117, June 12, 1995).

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

CHAPTER 2

PLANNING THE AUDIT

Planning is key to a quality audit, with the computer-related portion a significant part of the overall process. To be effective, the IS auditor and financial auditor should work together and coordinate information during this effort. Planning allows the auditor and senior members of the audit team to determine effective and efficient methods for obtaining evidential matter needed to assess an entity's computer-related controls. The nature, extent, and timing of planning vary according to the entity's size and complexity and the auditor's knowledge of the entity's operations.

Although concentrated at the beginning of an audit, planning is an iterative process performed throughout the audit. This is because the results of preliminary assessments provide the basis for determining the extent and type of subsequent testing. If auditors obtain evidence that specific control procedures are ineffective, they may find it necessary to reevaluate their earlier conclusions and other planning decisions made based on those conclusions.

During the planning phase, the auditor

- gains an understanding of the entity's operations and identifies the computer-related operations that are significant to the audit,
- assesses inherent risk and control risk,
- makes a preliminary assessment on whether general controls are likely to be effective, and
- identifies the general controls that will be tested.

The evaluation of computer-related controls should be planned in conjunction with other aspects of the audit. Detailed guidance on planning financial statement audits, including consideration of computer-related controls, is found in Section 200 of GAO's Financial Audit Manual. Appendix VI of this manual provides guidance for developing a multiyear audit strategy for entities with significant computer-related activities at multiple locations.

2.1 GAIN AN UNDERSTANDING OF THE ENTITY'S OPERATIONS AND IDENTIFY SIGNIFICANT COMPUTER-RELATED OPERATIONS

The auditor should first develop and document a high-level understanding of the entity or program operations being reviewed and how the entity/program is supported by automated systems. This should include obtaining an overview of each computer

application significant to the financial statements. Documentation of this understanding generally should include

- the significance and nature of the programs and functions supported by automated systems;
- the types of computer processing performed (stand alone, distributed, or networked);
- the specific hardware and software comprising the computer configuration, including (1) the type, number, and location of primary central processing units and peripherals, (2) the role of microcomputers, and (3) how such units are interconnected;
- the nature of software utilities used at computer processing locations that provide the ability to add, alter, or delete information stored in data files, databases, and program libraries;
- the nature of software used to restrict access to programs and data at computer processing locations;
- significant computerized communications networks, interfaces to other computer systems, and the ability to upload and/or download information;
- significant changes since any prior audits/reviews;
- the general types and extent of significant purchased software used;
- the general types and extent of significant software developed in-house;
- how (interactive or noninteractive) and where data are entered and reported;
- the approximate number of transactions processed by each significant system;
- the organization and staffing at the entity's data processing and software development sites, including recent key staff and organizational changes;
- the entity's reliance on service bureaus or other agencies for computer processing support; and
- results of past internal and external reviews, including those conducted by inspector general staff and consultants specializing in security matters.

Appendix I includes a Background Information Questionnaire that can be completed by agency managers in order to facilitate this initial audit step. Appendix II is a questionnaire for key system users to obtain an assessment of their satisfaction with significant computer applications and major computer outputs. This allows users to report problems and dissatisfactions that may affect the auditor's conclusions. Responses to the questionnaires should be reviewed and considered in the planning process.

2.2 ASSESS INHERENT RISK AND CONTROL RISK

After gaining an understanding of the entity's operations, the auditor assesses the inherent and control risks that are considered when determining audit risk, which is the risk that the auditor may unknowingly fail to appropriately modify an opinion on

financial statements that are materially misstated. Audit risk, as it relates to information systems, can be thought of in terms of the following three component risks:

- Inherent risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other impairment, assuming that there are no related internal controls.
- Control risk is the risk that a material misstatement in the entity's data will not be prevented or detected and corrected on a timely basis by the entity's internal control structure.
- Detection risk is the risk that the auditor will not detect a material misstatement in the financial statements.

On the basis of the level of audit risk and an assessment of the entity's inherent and control risks, the auditor determines the nature, timing, and extent of substantive audit procedures necessary to achieve the resultant detection risk. For example, in response to a high level of inherent and control risks, the auditor should perform additional audit procedures or more extensive substantive tests.

The auditor should (1) identify conditions that significantly increase inherent and control risks and (2) conclude whether they preclude the effectiveness of specific control techniques in significant applications. The auditor identifies specific inherent risks and control structure weaknesses based on information obtained in the planning phase, primarily from understanding the entity's operations. These factors are general in nature and require the auditor's judgment in determining (1) the extent of procedures to identify the risks and weaknesses and (2) the impact of such risks and weaknesses on the entity's operations and reports. Because this risk assessment requires the exercise of significant audit judgment, it should be performed by experienced audit team personnel.

For each inherent risk or control structure weakness identified, the auditor should document the nature and extent of the risk or weakness; the condition(s) that gave rise to that risk or weakness; and the specific information or operations affected (if not pervasive). The auditor should also document other considerations that may mitigate the effects of identified risks and weaknesses.

Factors Affecting Inherent Risk

The primary inherent risk factors that the auditor should consider are the nature of the entity's programs and accounts and any prior history of significant problems. For example, accounts involving subjective management judgments, such as loss allowances, are usually of higher risk than those involving objective determinations.

These factors are discussed in detail in Section 260.16 of GAO's Financial Audit Manual.

Computerized operations can introduce additional inherent risk factors not present in a manual system. The auditor should (1) consider each of the following factors and (2) assess the overall impact of computer processing on inherent risk. The impact of these factors typically will be pervasive in nature.

- **Uniform processing of transactions:** Because computers process groups of identical transactions consistently, any misstatements arising from erroneous computer programming will occur consistently in similar transactions. However, the possibility of random processing errors is reduced substantially in computer-based accounting systems.

- **Automatic processing:** The computer system may automatically initiate transactions or perform processing functions. Evidence of these processing steps (and any related controls) may or may not be visible.

- **Increased potential for undetected misstatements:** Computers use and store information in electronic form and require less human involvement in processing than manual systems. This increases the potential for individuals to gain unauthorized access to sensitive information and to alter data without visible evidence. Due to the electronic form, changes to computer programs and data are not readily detectible. Also, users may be less likely to challenge the reliability of computer output than manual reports.

- **Existence, completeness, and volume of the audit trail:** The audit trail is the evidence that demonstrates how a specific transaction was initiated, processed, and summarized. For example, the audit trail for a purchase could include a purchase order; a receiving report; an invoice; an entry in an invoice register (purchases summarized by day, month, and/or account); and general ledger postings from the invoice register. Some computer systems are designed to maintain the audit trail for only a short period, only in an electronic format, or only in summary form. Also, the information generated may be too voluminous to analyze effectively. For example, one transaction may result from the automatic summarization of information from hundreds of locations. Without the use of audit or retrieval software, tracing transactions through the processing may be extremely difficult.

- **Nature of the hardware and software used:** The nature of the hardware and software can affect inherent risk, as illustrated below.

    - The type of computer processing (on-line, batch oriented, or distributed)

presents different levels of inherent risk. For example, the inherent risk of unauthorized transactions and data entry errors may be greater for on-line processing than for batch-oriented processing.

- Peripheral access devices or system interfaces can increase inherent risk. For example, dial-up access to a system increases the system's accessibility to additional persons and therefore increases the risk of unauthorized access to computer resources.

- Distributed networks enable multiple computer processing units to communicate with each other, increasing the risk of unauthorized access to computer resources and possible data alteration. On the other hand, distributed networks may decrease the risk of data inconsistencies at multiple processing units through the sharing of a common database.

- Applications software developed in-house may have higher inherent risk than vendor-supplied software that has been thoroughly tested and is in general commercial use. On the other hand, vendor-supplied software new to commercial use may not have been thoroughly tested or undergone client processing to a degree that would encounter existing flaws.

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

Internal Control Components Affect Control Risk

In August 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[3] identified the following five interrelated components of internal control. These were adopted by the AICPA under Statement on Auditing Standards

[3] Internal Control--An Integrated Framework, August 1992. The Treadway Commission (The National Commission on Fraudulent Financial Reporting) was created in 1985 by the joint sponsorship of the American Institute of Certified Public Accountants, the American Accounting Association, the Financial Executives Institute, the Institute of Internal Auditors, and the Institute of Management Accountants.

(SAS) No. 78.[4] They were also incorporated into the January 1995 JFMIP publication, Framework for Federal Financial Management Systems, and into GAO's Internal Control: Standards for Internal Control in the Federal Government.

- The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; and the way management assigns authority and organizes and develops its people.

- Risk assessment is the identification and analysis of relevant risks to the achievement of the entity's objectives, forming a basis for determining how the risks should be managed.

- Control activities are the policies and procedures that help ensure that management directives are carried out. They include a range of activities including approvals, verifications, reconciliations, reviews of operating performance, and segregation of duties.

- Information and communication involves identifying, capturing, and communicating pertinent information to individuals in a form and time frame that enables them to carry out their responsibilities. This includes the information systems, methods, and records established to record, process, summarize, and report entity transactions.

- Monitoring refers to the ongoing activities that assess internal control performance over time and ensure that identified deficiencies are reported to senior management.

For financial statement audits, these elements will be assessed as they affect the effectiveness of an entity's overall internal control, including computer-related controls. When assessing the control environment, the auditor should also consider factors that are unique to computer-related operations. For example, the auditor should consider management's attitudes and awareness with respect to computerized operations. Management's interest in and awareness of computer functions and controls is important in establishing an organizationwide control consciousness. Management may demonstrate such interest and awareness by

- considering the risks and benefits of computer applications;

---

[4] Statement on Auditing Standards No. 78, Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS No. 55.

- communicating policies regarding computer functions and responsibilities;
- overseeing policies and procedures for developing, modifying, maintaining, and using computers and for controlling access to programs and files;
- considering the inherent and control risks related to computers and electronic data;
- responding to previous recommendations or concerns;
- quickly and effectively planning for, and responding to, computerized processing crises; and
- depending on but checking computer-generated information for key operating decisions.

The other internal control components--including risk assessment, control activities, communication, and monitoring--as they pertain to computer-related operations, are discussed in Chapter 3.

2.3 MAKE A PRELIMINARY ASSESSMENT ON WHETHER COMPUTER-RELATED CONTROLS ARE LIKELY TO BE EFFECTIVE

As part of assessing control risk, the auditor should make a preliminary assessment on whether computer-related controls are likely to be effective. This assessment is based primarily on discussions with personnel throughout the entity, including program managers, system administrators, information resource managers, and systems security managers; on observations of computer-related operations; and on cursory reviews of written policies and procedures.

During this phase, the auditor generally limits his or her understanding of controls to general controls at the overall entity level. However, obtaining this understanding usually requires visits to selected installations and discussions regarding major applications.

Tables listing control activities for critical elements in each general control category are provided in Chapter 3 and are summarized in Appendix III. The auditor can use the summary tables in Appendix III, which are also available in electronic form from GAO's World Wide Web server, to document his or her preliminary findings and to assist in making the preliminary assessment of controls. As the audit progresses through testing of internal controls, the auditor can continue to use the electronic version of the tables to document controls evaluated and tested, test procedures performed, conclusions, and supporting work paper references.

2.4 IDENTIFY CONTROLS TO BE TESTED

Based on the assessments of inherent and control risks, including the preliminary evaluation of computer-based controls, the auditor should identify the general control

techniques that appear most likely to be effective and that therefore should be tested to determine if they are in fact operating effectively. By relying on these preliminary assessments to plan audit tests, the auditor can avoid expending resources on testing controls that clearly are not effective. The tables in Appendix IV are provided for use in concluding the control effectiveness and for summarizing an overall assessment for each control category. These tables are also available in electronic form from GAO's World Wide Web server. (GAO's Internet address is: **<http://www.gao.gov>**.)

CHAPTER 3

EVALUATING AND TESTING GENERAL CONTROLS

3.0 OVERVIEW

General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. They create the environment in which application systems and controls operate. During a financial statement audit, the auditor will focus on general controls that normally pertain to an entity's major computer facilities and systems supporting a number of different applications, such as major data processing installations or local area networks. If general controls are weak, they severely diminish the reliability of controls associated with individual applications. For this reason, general controls are usually evaluated separately from and prior to evaluating application controls.

The auditor can often save time by anticipating needed audit work for general controls over specific applications and designing tests that address controls both at the entity or facility level and at the application level. For example, as part of the general controls evaluation, the auditor will test entitywide controls over computer program changes. If these controls appear to be effective, the auditor will then test program change controls for individual applications that are significant to the audit. By identifying these significant applications early, the auditor can design general control tests that include enough activity related to these applications to eliminate or reduce the need for separate application-level testing of general controls. (Testing of controls within significant applications is discussed in Chapter 4.)

There are six major categories of general controls that the auditor should consider. These are

- **entitywide security program planning and management** that provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls;

- **access controls** that limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure;

- **application software development and change controls** that prevent unauthorized programs or modifications to an existing program from being implemented;

- **system software** controls that limit and monitor access to the powerful programs and sensitive files that (1) control the computer hardware and (2) secure applications supported by the system;

- **segregation of duties** that are policies, procedures, and an organizational structure established so that one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records; and

- **service continuity** controls to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

For each of these six categories, the manual identifies several critical elements that represent tasks that are essential for establishing adequate controls. For each critical element, there is a discussion of the associated objectives, risks, and critical activities, as well as related control techniques and audit concerns. The auditor can use this information to evaluate entity practices.

For each critical element, the auditor should make a summary determination as to the effectiveness of the entity's related controls. If the controls for one or more of each category's critical elements are ineffective, then the controls for the entire category are not likely to be effective. The auditor should use professional judgment in making such determinations.

To facilitate the auditors' evaluation, tables identifying commonly used control techniques and related suggested audit procedures are included after the discussion of each critical element and are summarized in Appendix III. These tables can be used for both the preliminary evaluation and the more detailed evaluation and testing of controls. For the preliminary evaluation, the auditor can use the tables to guide and document his or her preliminary inquiries and observations. For the more detailed evaluation and testing, the auditor can use the suggested audit procedures in developing and carrying out a testing plan. Such a plan would include more extensive inquiries; inspections of facilities, systems, and written procedures; and tests of key control techniques, which may include using audit or system software and attempts to penetrate the system. To help document these evaluations and allow steps to be tailored to individual audits, electronic versions of the tables are available from GAO's World Wide Web server at the following Internet address: **<http://www.gao.gov>**.

3.1 ENTITYWIDE SECURITY PROGRAM PLANNING AND MANAGEMENT (SP)

An entitywide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

Through the Computer Security Act of 1987, the Congress provided a means for establishing minimum acceptable security practices related to federal computer systems. This act requires agencies to identify and protect systems containing "sensitive" information and calls for a computer standards program and security training. OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, as revised in February 1996, established a minimum set of controls for agencies' automated information security programs, including assigning responsibility for security, security planning, periodic review of security controls, and management authorization of systems to process information.

Comprehensive guidance on planning and managing an entitywide security program is contained in (1) NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, which provides guidance on security-related management, operational, and technical controls; and (2) GAO's executive guide describing risk management principles found at leading organizations, which is discussed in the following section.[1]

Risk Management Principles for an Effective Security Program

GAO studied nonfederal leading organizations that had reputations for having superior security programs to identify common principles and practices. The organizations had all embraced five risk management principles that were linked in a cycle of activity that helped ensure that information security policies addressed current risks on an ongoing basis. These principles are

---

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

- assess risk and determine needs,
- establish a central management focal point,
- implement appropriate policies and related controls,
- promote awareness, and
- monitor and evaluate policy and control effectiveness.

The organizations also had 16 common practices that were linked to these principles. The practices and associated principles are listed in Appendix VIII. This appendix also lists principles and an implementation approach for managing information security that were identified by the Information Technology Committee of the International Federation of Accountants.

Critical Elements Affect Internal Control Components

The critical elements in developing and implementing an entitywide security program involve factors that are essential to several internal control components, including the control environment. (See pages 2-5 and 2-6 for a discussion on internal control components.) Therefore, these critical elements help ensure the effectiveness of the entity's overall internal control. The relevant factors include supportive attitudes and actions by senior management, ongoing assessments of risk and monitoring of related policies, and effective communications between management and staff. All internal control components should be present and functioning effectively to conclude that internal control is effective. However, the control environment sets the tone of the organization. Generally, a specific control technique or group of techniques cannot be relied on to be effective on an ongoing basis unless it is supported by a strong control environment. For this reason, the auditor should be cognizant of control environment factors throughout the audit and adjust audit procedures accordingly.

Assessing an entitywide security program involves evaluating the entity's efforts to perform each of the following critical elements.

CRITICAL ELEMENTS

SP- 1 Periodically assess risks

SP- 2 Document an entitywide security program plan

SP- 3 Establish a security management structure and clearly assign security responsibilities

SP- 4 Implement effective security-related personnel policies

SP- 5 Monitor the security program's effectiveness and make changes as needed

Critical Element SP-1: Periodically assess risks

A comprehensive high-level risk assessment should be the starting point for developing or modifying an entity's security policies and plan. Such assessments are important because they help make certain that all threats and vulnerabilities are identified and considered, that the greatest risks are identified, and that appropriate decisions are made regarding which risks to accept and which to mitigate through security controls. The Federal Managers Financial Integrity Act of 1982 requires agencies to conduct risk assessments to identify and prioritize their vulnerabilities to waste, fraud, and abuse, and OMB Circular A-130, Appendix III, requires that agencies consider risk when determining the need for and selecting computer-related control techniques. However, this circular no longer requires formal periodic risk analyses that attempt to quantify in dollars an annual loss exposure resulting from unfavorable events.

Risk assessments should consider data sensitivity and the need for integrity and the range of risks that an entity's systems and data may be subject to, including those risks posed by authorized internal and external users, as well as unauthorized outsiders who may try to "break into" the systems. Such analyses should also draw on reviews of system and network configurations and observations and testing of existing security controls.

GAO's study of security programs at leading organizations found that the following were key factors for successful risk assessment programs. The organizations

- had a defined process that allowed an entitywide understanding of what a risk assessment was and avoided reinventing the wheel by individual units,
- required that risk assessments be performed and had designated a central security group to schedule them and facilitate their conduct,
- involved a mix of individuals with knowledge of business operations and technical aspects of the organization's systems and security controls,
- required some type of final sign-off by the business managers indicating agreement with risk reduction decisions and acceptance of the residual risk,
- required that final documentation be forwarded to more senior officials and to internal auditors so that participants could be held accountable for their decisions, and

- did not attempt to precisely quantify risk. Although they would have liked to place a dollar value on risks and precisely quantify the costs and benefits of controls, they felt that spending time on such an exercise was not worth the trouble. They believed there was little reliable data on either the actual frequency of security incidents or on the full costs of controls and of damage due to a lack of controls.

Risk assessments can also benefit when they include personnel with enough independence to be objective. Risk assessment and risk management are ongoing efforts. Although a formal comprehensive risk assessment may be performed periodically--every several years--risk should be considered whenever there is a change in the entity's operations or its use of technology or in outside influences affecting its operations.

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

Control Activities	Control Techniques	Audit Procedures
Risks are periodically assessed.	Independent risk assessments are performed and documented on a regular basis or whenever systems, facilities, or other conditions change. The risk assessment considers data sensitivity and integrity and the range of risks to the entity's systems and data. Final risk determinations and related management approvals are documented and maintained on file. (Such determinations may be incorporated in the security program plan, which is discussed in the next section.)	Review risk assessment policies. Review the most recent high-level risk assessment. Review the objectivity of personnel who performed and reviewed the assessment.

Critical Element SP-2: Document an entitywide security program plan

Entities should have a written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security (the security management function) as well as those who own, use, or rely on the entity's computer resources.

The Computer Security Act requires federal agencies to develop and implement plans to safeguard systems that maintain sensitive data. The act defines "sensitive" information as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under [the Privacy Act.]" The Privacy Act requires that personal information about individuals stored in federal recordkeeping systems be kept confidential. Also, OMB Circular A-130, Appendix III, provides specific guidance on what should be covered in agency system security plans.

SP-2.1: A security plan is documented and approved

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

To help ensure that the plan is complete and supported by the entity as a whole, senior management should obtain agreement from all affected parties in establishing policies for a security program. Such agreements will also help ensure that policies and procedures for security developed at lower levels within the organization are consistent with overall organizational policies and procedures. In accordance with OMB Circular A-130, Appendix III, final responsibility for determining that the plan provides for reducing risk to an acceptable level should lie with the manager whose program operations and assets are at risk. However, any disagreements between program managers and security specialists as to the adequacy of policies and controls should be resolved by senior management. This manual addresses separately access controls and continuity of service under sections 3.2 and 3.6, respectively.

Security Controls to Include in Entity Security Plans	
General Support System	**Major Application**
Rules of the system[a]	Application rules[a]
Training	Specialized training
Personnel controls	Personnel security
Incident response capability	--
Continuity of support	Contingency planning
Technical security	Technical controls
System interconnection	Information sharing
--	Public access controls

[a]This includes delineating responsibilities and expected behavior.

SP-2.2: The plan is kept current

To be effective, the policies and plan should be maintained to reflect current conditions. They should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk due to factors such as changes in agency mission or the types and configuration of computer resources in use. Revisions to the plan should be reviewed, approved, and communicated to all employees. Outdated policies and plans not only reflect a lack of top management concern, but also may not address current risks and, therefore, may be ineffective.

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

Control Activities	Control Techniques	Audit Procedures
SP-2.1 A security plan is documented and approved.	A security program plan has been documented that • covers all major facilities and operations, • has been approved by key affected parties, and • covers the topics prescribed by OMB Circular A-130 (general support systems/major applications) •Rules of the system / Application rules •Training / Specialized training •Personnel controls / Personnel security •Incident response capability / - - •Continuity of support / Contingency planning •Technical security / Technical controls •System interconnection / Information sharing • - - / Public access controls	Review the security plan. Determine whether the plan covers the topics prescribed by OMB Circular A-130.
SP-2.2 The plan is kept current.	The plan is reviewed periodically and adjusted to reflect current conditions and risks.	Review the security plan and any related documentation indicating that it has been reviewed and updated and is current.

Critical Element SP-3: Establish a security management structure and clearly assign security responsibilities

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

SP-3.1: A security management structure has been established

The effectiveness of the security program is affected by the way in which responsibility for overseeing its implementation is assigned. Generally, such responsibility is assigned to a central security program office. Our survey of leading organizations found that a central management focal point is key to ensuring that the various activities associated with managing risks are carried out. (See Appendix VIII.) The central group may be supplemented by individual security program officers, designated in units within the entity who assist in the implementation and management of the organization's security program. These individual unit security officers should report to or coordinate with the central security program office.

Responsibilities of the central security program office may include

- facilitating risk assessments,
- coordinating the development of and distributing security policies and procedures,
- routinely monitoring compliance with these policies,
- promoting security awareness among system users,
- providing reports to senior management on policy and control evaluation results and advice to senior management on security policy-related issues, and
- representing the entity in the security community.

In assessing the effectiveness of the security management structure, the auditor should consider the security function's scope of authority, placement, training and experience, and tools. For example, security management personnel should

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

SP-3.2: Information security responsibilities are clearly assigned

OMB Circular A-130, Appendix III, requires that the rules of the system and application "shall clearly delineate responsibilities and expected behavior of all individuals with access. . .and shall be clear about the consequences of behavior not consistent with the rules." Security-related responsibilities of offices and individuals throughout the entity that should be clearly defined include those of (1) information resource owners and users, (2) information resources management and data processing personnel, (3) senior management, and (4) security administrators. Further, responsibilities for individual employee accountability regarding the use and disclosure of information resources should be established.

The security plan should clearly establish who "owns" the various computer resources, especially data files, and what the responsibilities of ownership are. Ownership of computer resources should be assigned to persons responsible for their reliability and integrity. For example, owners of data files and application programs are generally the managers of the programs supported by these applications. These managers are primarily responsible for the proper operation of the program and for accurate reporting of related computer data. Similarly, owners of computer facilities and equipment are generally managers who are responsible for the physical protection of these resources. If a resource has multiple owners, policies should clearly describe whether and how ownership responsibilities are to be shared.

Assignment of ownership responsibilities is important because the managers who own the resources are in the best position to (1) determine their sensitivity, (2) analyze the duties and responsibilities of users, and (3) determine the specific access needs of these users. Once these factors are determined, the resource owner can identify persons authorized to have access to the resource and the extent of such access. The

owners should communicate these authorizations to the security function, which is then responsible for implementing access controls in accordance with the owners' authorizations. Section 3.2 - Access Control discusses access authorization further.

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

SP-3.3: Owners and users are aware of security policies

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

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

The Computer Security Act specifically requires each agency to provide "mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency." Also, OMB Circular A-130, Appendix III, requires training of individuals before granting access to systems or applications. The training is to make sure they are aware of the system or application rules, their responsibilities, and their expected behavior.

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

SP-3.4: An incident response capability has been implemented

OMB Circular A-130, Appendix III, points out that security incidents--whether caused by viruses, hackers, or software bugs--are becoming more common. Also, they are of more concern because as systems are increasingly interconnected, security incidents can place many valuable resources at risk of corruption or disclosure. Therefore, Appendix III requires agencies to establish formal incident response mechanisms and to make system users aware of these mechanisms and how to use them. Appendix III also tasks the National Institute of Standards and Technology (NIST) with coordinating activities governmentwide for agencies sharing information concerning common vulnerabilities and threats. Appendix III also directs the Department of Justice to provide appropriate guidance on pursuing legal remedies in the case of serious incidents.

According to NIST, the two main benefits of an incident handling capability are (1) containing and repairing damage from incidents and (2) preventing future damage. One category of incidents is virus infection. NIST views virus identification software as an important tool to help contain damage from viruses.

There are also a number of less obvious side benefits from an incident handling capability, which include

- improved threat data for use in the risk assessment and control selection process,
- enhanced internal communication and organization preparedness, and
- enhanced training and awareness programs by providing trainers better information on users' knowledge and providing real-life illustrations for classes.

Also, according to NIST, the characteristics of a good incident handling capability are

- an understanding of the constituency being served, including computer users and program managers;
- an educated constituency that trusts the incident handling team;
- a means of prompt centralized reporting, such as through a hotline;
- a response team with necessary knowledge, skills, and abilities, including technical expertise with the computer technology used by the organization, and the ability and willingness to respond when needed, where needed; and
- links to other groups--such as law enforcement agencies, response teams, or security groups external to the organization--and to the organization's public relations office (in case the incident received media attention).

One aspect of incident response that can be especially problematic is gathering the evidence to pursue legal action. In order to gather evidence, an organization may

need to allow an intruder or violator to continue his or her inappropriate activities--a situation that puts the system and data at continued risk. However, fear of detection and prosecution can serve as a deterrent to future violations.

To provide a federal governmentwide incident response capability, NIST initiated the Federal Computer Incident Response Capability (FedCIRC) Program, which became operational in October 1996. FedCIRC provides agencies with cost-reimbursable, direct technical assistance and incident handling support, as well as a forum for sharing information on incidents, threats, and vulnerabilities. (As of March 1998, the CIO Council was exploring ways to encourage broader use of FedCIRC.)

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

Control Activities	Control Techniques	Audit Procedures
SP-3.1 A security management structure has been established.	The security program plan establishes a security management structure with adequate independence, authority, and expertise.	Review the security plan and the entity's organization chart. Interview security management staff.
	An information systems security manager has been appointed at an overall level and at appropriate subordinate levels.	Review pertinent organization charts and job descriptions. Interview the security manager.
SP-3.2 Information security responsibilities are clearly assigned.	The security plan clearly identifies who owns computer-related resources and who is responsible for managing access to computer resources. Security responsibilities and expected behaviors are clearly defined for (1) information resource owners and users, (2) information resources management and data processing personnel, (3) senior management, and (4) security administrators.	Review the security plan.
SP-3.3 Owners and users are aware of security policies.	An ongoing security awareness program has been implemented. It includes first-time training for all new employees, contractors, and users, and periodic refresher training thereafter.	Review documentation supporting or evaluating the awareness program. Observe a security briefing. Interview data owners and system users. Determine what training they have received and if they are aware of their security-related responsibilities.
	Security policies are distributed to all affected personnel, including system/application rules and expected behaviors.	Review memos, electronic mail files, or other policy distribution mechanisms. Review personnel files to test whether security awareness statements are current. Call selected users, identify yourself as security or network staff, and attempt to talk them into revealing their password.
SP-3.4 An incident response capability has been implemented.	The entity's incident response capability has characteristics suggested by NIST: • use of virus identification software, • an understanding of the constituency being served, • an educated constituency that trusts the incident handling team, • a means of prompt centralized reporting, • response team members with the necessary knowledge, skills, and abilities, and • links to other relevant groups.	Interview security manager, response team members, and system users. Review documentation supporting incident handling activities. Determine qualifications of response team members. *(Note: See also Section 3.2, Critical Element AC-4 on monitoring access and security violations.)*

Critical Element SP-4: Implement effective security-related personnel policies

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

SP-4.1: Hiring, transfer, termination, and performance policies address security

The security plan should include policies related to the security aspects of hiring, terminating, and transferring employees and assessing their job performance. Procedures that should generally be in place include the following:

- Hiring procedures should include contacting references and background investigations and periodic reinvestigations are performed at least once every 5 years, consistent with the sensitivity of the position per criteria from the Office of Personnel Management.
- For employees and contractors assigned to work with confidential information, there should be confidentiality or security agreements that specify precautions required and unauthorized disclosure acts, contractual rights, and obligations during employment and after termination.
- Periodic job rotations and vacations should be mandatory, and work should be temporarily reassigned during vacations.
- Performance ratings for individual employees should cover compliance with security policies and procedures.
- Compensation and recognition should be appropriate to promote high morale.
- Termination and transfer procedures should include

    - exit interview procedures;
    - return of property, such as keys, identification cards, badges, and passes;
    - notification to security management of terminations, and prompt termination of access to the entity's resources and facilities (including passwords);

- immediately escorting terminated employees--especially those who have access to sensitive resources--out of the entity's facilities; and
- identifying the period during which nondisclosure requirements remain in effect.

SP-4.2: Employees have adequate training and expertise

Management should ensure that employees--including data owners, system users, data processing personnel, and security management personnel--have the expertise to carry out their information security responsibilities. To accomplish this, the security program should include

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

Control Techniques and Suggested Audit Procedures for Critical Element SP-4		
Control Activities	**Control Techniques**	**Audit Procedures**
SP-4.1 Hiring, transfer, termination, and performance policies address security.	For prospective employees, references are contacted and background checks performed.	Review hiring policies. For a selection of recent hires, inspect personnel records and determine whether references have been contacted and background checks have been performed.
	Periodic reinvestigations are performed at least once every 5 years, consistent with the sensitivity of the position per criteria from the Office of Personnel Management.	Review reinvestigation policies. For a selection of sensitive positions, inspect personnel records and determine whether background reinvestigations have been performed.
	Confidentiality or security agreements are required for employees and contractors assigned to work with confidential information.	Review policies on confidentiality or security agreements. For a selection of such users, determine whether confidentiality or security agreements are on file.
	Regularly scheduled vacations exceeding several days are required, and the individual's work is temporarily reassigned.	Review vacation policies. Inspect personnel records to identify individuals who have not taken vacation or sick leave in the past year. Determine who performed vacationing employee's work during vacation.
	Regular job or shift rotations are required.	Review job rotation policies. Review staff assignment records and determine whether job and shift rotations occur.
	Termination and transfer procedures include • exit interview procedures; • return of property, keys, identification cards, passes, etc.; • notification to security management of terminations and prompt revocation of IDs and passwords; • immediately escorting terminated employees out of the entity's facilities; and • identifying the period during which nondisclosure requirements remain in effect.	Review pertinent policies and procedures. For a selection of terminated or transferred employees, examine documentation showing compliance with policies. Compare a system-generated list of users to a list of active employees obtained from personnel to determine if IDs and passwords for terminated employees exist.

Control Techniques and Suggested Audit Procedures for Critical Element SP-4		
Control Activities	**Control Techniques**	**Audit Procedures**
SP-4.2 Employees have adequate training and expertise.	Skill needs are accurately identified and included in job descriptions, and employees meet these requirements.	Review job descriptions for security management personnel and for a selection of other personnel. For a selection of employees, compare personnel records on education and experience with job descriptions.
	A training program has been developed.	Review training program documentation.
	Employee training and professional development are documented and monitored.	Review training records and related documentation showing whether such records are monitored and whether employees are receiving the appropriate training.

Critical Element SP-5: Monitor the security program's effectiveness and make changes as needed

An important element of risk management is ensuring that policies and controls intended to reduce risk are effective on an ongoing basis. Senior management's awareness, support, and involvement are essential in establishing the control environment needed to promote compliance with the entity's information security program. However, because security is not an end in itself, senior managers should balance the emphasis on security with the larger objective of achieving the entity's mission. To do this effectively, top management should understand the entity's security risks and actively support and monitor the effectiveness of the entity's security policies. If senior management does not monitor the security program, it is unlikely that others in the organization will be committed to properly implementing it.

SP-5.1: Management periodically assesses the appropriateness of security policies and compliance with them

To implement an effective security plan, top management should monitor its implementation and adjust the plan in accordance with changing risk factors. Over time, policies and procedures may become inadequate because of changes in operations or deterioration in the degree of compliance. Periodic assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan. Such assessments can be performed by agency staff or by external reviewers engaged by management. Independent audits performed or arranged by GAO and agency IGs, while an important check on management performance, should not be viewed as a substitute for management evaluations of the adequacy of the organization's security program.

OMB Circular A-130, Appendix III, requires that federal agencies review the security of their general support systems and major applications at least once every 3 years or sooner, if significant modifications have occurred or where the risk and magnitude of harm are high. Although not required by this circular, it would be appropriate for an agency to describe its evaluation program, including the expected type of testing and frequency of evaluations, in its security plan. (Security plans are discussed in critical element SP-2.)

The circular also requires that a management official authorize in writing the use of each general support system and major application. Some agencies refer to this authorization as accreditation. The circular allows self reviews of controls for general support systems, but requires an independent review or audit of major applications. The authorizations or accreditations are to be provided by the program or function managers whose missions are supported by the automated systems and represent the managers' explicit acceptance of risk based on the results of any security reviews, including those performed as part of financial statement audits and during related risk assessments. Additional guidance on accrediting federal automated systems can be found in Federal Information Processing Standard Publication 102, Guideline for Computer Security Certification and Accreditation, September 1983.

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

SP-5.2: Management ensures that corrective actions are effectively implemented

When significant weaknesses are identified, the related risks should be reassessed, appropriate corrective actions taken, and follow-up monitoring performed to make certain that corrective actions are effective. This is an important aspect of management's risk management responsibilities.

In addition to modifying written policies to correct identified problems, implementation of the corrective actions should be tested to see whether they are understood and are effective in addressing the problem. Management should continue to periodically review and test such corrective actions to see that they remain effective on a continuing basis.

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

Control Activities	Control Techniques	Audit Procedures
SP-5.1 Management periodically assesses the appropriateness of security policies and compliance with them.	The entity's IS security program is subjected to periodic reviews.	Review the reports resulting from recent assessments, including the most recent FMFIA report.
	Major applications undergo independent review or audit at least every 3 years.	Determine when last independent review or audit occurred and review results.
	Major systems and applications are authorized or accredited by the managers' whose missions they support.	Review written authorizations or accreditation statements.
	Top management initiates prompt action to correct deficiencies.	Review documentation related to corrective actions.
SP-5.2 Management ensures that corrective actions are effectively implemented.	Corrective actions are tested after they have been implemented and monitored on a continuing basis.	Review the status of prior-year audit recommendations and determine if implemented corrective actions have been tested. Review recent FMFIA reports.

Sources of Additional Information on Entitywide Security Programs

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

Information Systems Audit and Control Foundation, CobiT: Control Objectives for Information *and* Related Technology, 1998.

Information Technology Committee, International Federation of Accountants, Managing Security of Information and Communications, Exposure Draft, June 1997.

NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, December 1996.

Office of Management and Budget (OMB) Circular A-130, Revised February 8, 1996, (Transmittal Memorandum No. 3), Appendix III, Security of Federal Automated Information Resources.

NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, December 1995.

Lainhart and Donahue, The Information Systems Control Foundation, Computerized Information Systems (CIS) Audit Manual: A Guide to CIS Auditing in Government Organizations, July 1992.

The Institute of Internal Auditors Research Foundation, Systems Auditability and Control: Module 9 - Security, April 1991.

NIST Special Publication 500-172, Computer Security Training Guidelines, November 1989.

The Computer Security Act of 1987.
(P.L. 100-235, 40 U.S.C. 759 note)

FIPS 102, Computer Security Certification and Accreditation, September 27, 1983.

The Federal Managers' Financial Integrity Act of 1982.
(P.L. 97-255, 31 U.S.C. 3512)

The Privacy Act of 1974, as Amended.
(P.L. 93-579, 5 U.S.C. 552a)

3.2 ACCESS CONTROL (AC)

Access controls should provide reasonable assurance that computer resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. Such controls include physical controls, such as keeping computers in locked rooms to limit physical access, and logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files.

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

- By obtaining direct access to data files, an individual could make unauthorized changes for personal gain or obtain sensitive information. For example, a person could (1) alter the address of a payee and thereby direct a disbursement to himself or herself, (2) alter inventory quantities to conceal a theft of assets, (3) inadvertently or purposefully change a receivable balance, or (4) obtain confidential information about business transactions or individuals.
- By obtaining access to application programs used to process transactions, an individual could make unauthorized changes to these programs or introduce malicious programs, which in turn could be used to access data files, resulting in situations similar to those described above, or to process unauthorized transactions. For example, a person could alter a payroll or payables program to inappropriately generate a check for himself or herself.
- By obtaining access to computer facilities and equipment, an individual could (1) obtain access to terminals or telecommunications equipment that provide input into the computer, (2) obtain access to confidential or sensitive information on magnetic or printed media, (3) substitute unauthorized data or programs, or (3) steal or inflict malicious damage on computer equipment and software.

The objectives of limiting access are to ensure that

- users have only the access needed to perform their duties,
- access to very sensitive resources, such as security software programs, is limited to very few individuals, and
- employees are restricted from performing incompatible functions or functions beyond their responsibility. (Segregation of duties is discussed in greater detail in Section 3.5.)

If these objectives are met, the risk of inappropriate modification or disclosure of data can be reduced without interfering with the practical needs of users. However,

establishing the appropriate balance between user needs and security requires a careful analysis of the criticality and sensitivity of information resources available and the tasks performed by users.

Implementing adequate access controls involves first determining what level and type of protection is appropriate for individual resources and who needs access to these resources. These tasks should be performed by the resource owners. For example, program managers should determine how valuable their program data resources are and what access is appropriate for personnel who must use an automated system to carry out, assess, and report on program operations. Similarly, managers in charge of system development and modification should determine the sensitivity of hardware and software resources under their control and the access needs of systems analysts and programmers, and system administration officials should determine the access needs of system administration personnel.

Assessing access controls involves evaluating the entity's success in performing each of the critical elements listed below.

CRITICAL ELEMENTS

AC-1 Classify information resources according to their criticality and sensitivity

AC-2 Maintain a current list of authorized users and their access authorized

AC-3 Establish physical and logical controls to prevent or detect unauthorized access

AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action

Critical Element AC-1: Classify information resources according to their criticality and sensitivity

To protect resources adequately with the most cost-effective means, owners should first determine the level of protection needed. While virtually all information resources merit some level of protection, the most critical resources should be subject to the strongest protective controls. However, there are costs associated with procuring, implementing, and maintaining protective controls. In addition, such controls often reduce efficiency since they require employees to perform additional steps to access and use data and resources. For this reason, an entity should generally strive to provide an adequate level of protection, given the specific risks involved, and an understanding of the costs and benefits associated with the protection. The costs of protection should not exceed the benefits derived.

AC-1.1: Resource classifications and related criteria have been established

Policies specifying classification categories and related criteria can help resource owners classify their resources according to their need for protective controls. The Computer Security Act requires agencies to identify systems that process "sensitive" data, defined as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under [the Privacy Act.]" OMB Circular A-130, Appendix III, directs federal agencies to assume that all major systems contain some sensitive information that needs to be protected, but to focus extra security controls on a limited number of particularly high-risk or major applications.

To select the most appropriate controls, entities should develop classification categories that meet their legal and business requirements for confidentiality, integrity, and availability. For example, it may be important to protect both the confidentiality and integrity of some files while, for others, only integrity may be a concern. Classifications may also involve hierarchical security levels, such as minimally sensitive, moderately sensitive, and highly sensitive. The most important factors are that the classifications be carefully formulated and based on the risks involved.

AC-1.2: Owners have classified resources

Resource owners should determine which classifications are most appropriate for the resources for which they are responsible. These determinations should flow directly

from the results of risk assessments that identify threats, vulnerabilities, and the potential negative effects that could result from disclosing confidential data or failing to protect the integrity of data supporting critical transactions or decisions. All resource classifications should be reviewed and approved by an appropriate senior official, maintained on file, and periodically reviewed to ensure that they reflect current conditions.

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

Control Activities	Control Techniques	Audit Procedures
AC-1.1 Resource classifications and related criteria have been established.	Classifications and criteria have been established and communicated to resource owners.	Review policies and procedures. Interview resource owners.
AC-1.2 Owners have classified resources.	Resources are classified based on risk assessments; classifications are documented and approved by an appropriate senior official and are periodically reviewed.	Review resource classification documentation and compare to risk assessments. Discuss any discrepancies with appropriate officials.

Critical Element AC-2: Maintain a current list of authorized users and their access authorized

An entity should institute policies and procedures for authorizing access to information resources and documenting such authorizations. These policies and procedures should cover user access needed for routine operations, emergency access, and the sharing and disposition of data with individuals or groups outside the entity.

AC-2.1: Resource owners have identified authorized users and their access authorized

The computer resource owner should identify the specific user or class of users that are authorized to obtain direct access to each resource for which he or she is responsible. This process can be simplified by developing standard profiles, which describe access needs for groups of users with similar duties, such as accounts payable clerks.

The owner should also identify the nature and extent of access to each resource that is available to each user. This is referred to as the user's profile. In general, users may be assigned one or more of the following types of access to specific computer resources:

- Read access, which is the ability to look at and copy data or a software program.
- Update access, which is the ability to change data or a software program.
- Delete access, which is the ability to erase or remove data or programs.
- Merge access, which is the ability to combine data from two separate sources.
- Execute access, which is the ability to execute a software program.

Access may be permitted at the file, record, or field level. Files are composed of records, typically one for each item or transaction. Individual records are composed of fields that contain specific data elements relating to each record. Access authorizations should be documented on standard forms, maintained on file, approved by senior managers, and securely transferred to security managers. Owners should periodically review access authorization listings and determine whether they remain appropriate.

Broad or special access privileges, such as those associated with operating system software that allow normal controls to be overridden, are only appropriate for a small number of users who perform system maintenance or handle emergency situations.

Such special privileges may be granted on a permanent or temporary basis. However, any such access should also be approved by a senior security manager, written justifications should be kept on file, and the use of highly sensitive files or access privileges should be closely monitored by management.

Also, for systems that can be accessed through public telecommunications lines, some users may be granted dial-up access. This means that these individuals can use a modem to access and use the system from a remote location, such as their home or a field office. Because such access can significantly increase the risk of unauthorized access, it should be limited and the associated risks weighed against the benefits. To help manage the risk of dial-up access, justification for such access should be documented and approved by owners. (See section AC-3.2 for additional controls to help manage the risk of dial-up access, such as dial-back procedures to preauthorized phone numbers or the use of security modems, tokens, or smart cards to authenticate a valid user.)

Listings of authorized users and their specific access needs and any modifications should be approved by an appropriate senior manager and directly communicated in writing by the resource owner to the security management function. A formal process for transmitting these authorizations, including the use of standardized access request forms, should be established to reduce the risk of mishandling, alterations, and misunderstandings. The security manager should review authorizations for new or modified access privileges and discuss any questionable authorizations with the authorizing official. Approved authorizations should be maintained on file.

It is equally important to notify the security function immediately when an employee is terminated or, for some other reason, is no longer authorized access to information resources. Notification may be provided by the human resources department or by others, but policies should be in place that clearly assign responsibility for such notifications. Terminated employees who continue to have access to critical or sensitive resources pose a major threat, especially those individuals who may have left under acrimonious circumstances.

Compliance with access authorizations should be monitored by periodically comparing authorizations to actual access activity. Access control software typically provides a means of reporting user access authorizations and access activity.

AC-2.2: Emergency and temporary access authorization is controlled

Occasionally, there will be a need to grant temporary access privileges to an individual who is not usually authorized access. Such a need may arise during emergency situations, when an individual is temporarily assigned duties that require access to critical or sensitive resources, or for service or maintenance personnel. In

addition, contractor personnel may require temporary access while doing system development or other work.

As with normal access authorizations, temporary access should be approved and documented and the related documentation maintained on file. Also, temporary user identifications and authentication devices, such as passwords, should be designed to automatically expire after a designated date.

AC-2.3: Owners determine disposition and sharing of data

A mechanism should be established so that the owners of data files and programs determine whether and when these resources are to be maintained, archived, or deleted. Standard disposition forms can be used and maintained on file to document the users' approvals.

In addition, resource owners should determine if, with whom, and by what means information resources can be shared. When files are shared with other entities, it is important that (1) data owners understand the related risks and approve such sharing and (2) receiving entities understand the sensitivity of the data involved and safeguard the data accordingly. This should normally require a written agreement prior to the sharing of sensitive information.

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

Control Activities	Control Techniques	Audit Procedures
AC-2.1 Resource owners have identified authorized users and their access authorized.	Access authorizations are • documented on standard forms and maintained on file, • approved by senior managers, and • securely transferred to security managers.	Review pertinent written policies and procedures. For a selection of users (both application user and IS personnel) review access authorization documentation.
	Owners periodically review access authorization listings and determine whether they remain appropriate.	Interview owners and review supporting documentation. Determine whether inappropriate access is removed in a timely manner.
	The number of users who can dial into the system from remote locations is limited and justification for such access is documented and approved by owners. (See section AC-3.2 for additional controls over dial-up access.)	For a selection of users with dial-up access, review authorization and justification.
	Security managers review access authorizations and discuss any questionable authorizations with resource owners.	Interview security managers and review documentation provided to them.

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

Control Activities	Control Techniques	Audit Procedures
AC-2.1 Resource owners have identified authorized users and their access authorized. (continued)	All changes to security profiles by security managers are automatically logged and periodically reviewed by management independent of the security function. Unusual activity is investigated.	Review a selection of recent profile changes and activity logs.
	Security is notified immediately when system users are terminated or transferred.	Obtain a list of recently terminated employees from Personnel and, for a selection, determine whether system access was promptly terminated.
AC-2.2 Emergency and temporary access authorization is controlled.	Emergency and temporary access authorizations are • documented on standard forms and maintained on file, • approved by appropriate managers, • securely communicated to the security function, and • automatically terminated after a predetermined period.	Review pertinent policies and procedures. Compare a selection of both expired and active temporary and emergency authorizations (obtained from the authorizing parties) with a system-generated list of authorized users. Determine the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed.
AC-2.3 Owners determine disposition and sharing of data.	Standard forms are used to document approval for archiving, deleting, or sharing data files.	Examine standard approval forms. Interview data owners.
	Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.	Examine documents authorizing file sharing and file sharing agreements.

Critical Element AC-3: Establish physical and logical controls to prevent or detect unauthorized access

The entity should have a cost-effective process for protecting data files, application programs, and hardware through a combination of physical and logical security controls. Physical security involves restricting physical access to computer resources, usually by limiting access to the buildings and rooms where they are housed, or by installing locks on computer terminals. However, physical controls alone cannot ensure that programs and data are protected. For this reason, it is important to establish logical security controls that protect the integrity and confidentiality of sensitive files. The security function should be responsible for implementing and maintaining both physical and logical controls based upon authorizations provided by the owners of the resources.

Cryptographic tools help provide access control by rendering data unintelligible to unauthorized users and/or protecting the integrity of transmitted or stored data. Currently, cryptographic tools are not widely used by federal agencies. However, they are especially useful in network environments and their use is likely to increase to include providing electronic signatures that help authenticate messages and ensure the integrity of files.

Assessing the effectiveness of physical and logical controls can involve highly technical issues, especially for large integrated systems and systems that involve telecommunications. For this reason, even an experienced IS auditor may need to seek technical advice from an expert on some issues.

AC-3.1: Adequate physical security controls have been implemented

Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. Computer resources to be protected include

- primary computer facilities,
- cooling system facilities,
- terminals that are used to access a computer,
- microcomputers,

- computer file storage areas, and
- telecommunications equipment and lines, including wiring closets.

A. Physical safeguards have been established that are commensurate with the risks of physical damage or access

To evaluate the effectiveness of physical security controls, the auditor should consider whether the entity has

- identified all sensitive areas--such as buildings, individual rooms or equipment, software and tape libraries, or telecommunication lines--that are susceptible to physical access, loss, or impairment;
- identified all physical access points and threats to all sensitive areas; and
- developed cost-effective security controls over all physical access points and addressed all significant threats to sensitive areas.

Access should be limited to personnel with a legitimate need for access to perform their duties. Management should regularly review the list of persons authorized to have physical access to sensitive facilities.

Physical security controls vary, but may include

- manual door or cipher key locks,
- magnetic door locks that require the use of electronic keycards,
- biometrics authentication,
- security guards,
- photo IDs,
- entry logs,
- logs and authorization for removal and return of tapes and other storage media to the library,
- electronic and visual surveillance systems,
- perimeter fences around sensitive buildings,
- perimeter intrusion alarms, and
- computer terminal locks.

The auditor should consider whether surreptitious entry into sensitive facilities is possible. For example, could unauthorized persons gain entry by

- observing lock combinations entered by authorized personnel,
- obtaining unsecured keycards,

- going over the top of a partition that stops at the underside of a suspended ceiling when the partition serves as a wall for a sensitive facility, or
- cutting a hole in a plasterboard wall in a location hidden by furniture.

Physical controls also include environmental controls, such as smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies. However, because these controls tend to pertain to unexpected disruptive events rather then access control, they are discussed in section 3.6--Service Continuity.

In evaluating the effectiveness of physical security controls, the auditor should consider the effectiveness of the entity's policies and practices for

- granting and discontinuing access authorizations,
- controlling passkeys,
- controlling entry during and after normal business hours.
- controlling the deposit and withdrawals of tapes and other storage media to and from the library,
- handling emergencies,
- controlling reentry after emergencies, and
- establishing compensatory controls when restricting physical access is not feasible, as is often the case with telecommunications lines.

B. Visitors are controlled

On occasion, persons other than regularly authorized personnel may be granted access to sensitive areas or facilities, such as employees from another entity facility, maintenance personnel, contractors, and the infrequent or unexpected visitor. All of these visitors should be controlled and not be granted unrestricted access. Controls should include

- preplanned appointments,
- identification checks,
- controlling the reception area,
- logging in visitors,
- escorting visitors while in sensitive areas, and
- periodically changing entry codes to prevent reentry by previous visitors who might have become knowledgeable of the code.

AC-3.2: Adequate logical access controls have been implemented

Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user identification numbers (IDs), passwords, or other identifiers that are linked to predetermined access privileges. Logical controls should be designed to restrict legitimate users to the specific systems, programs, and files that they need and prevent others, such as hackers, from entering the system at all.

Logical security controls enable the entity to

- identify individual users or computers that are authorized access to computer networks, data, and resources,
- restrict access to specific sets of data or resources,
- produce and analyze audit trails of system and user activity, and
- take defensive measures against intrusion.

To evaluate the effectiveness of logical security controls, the IS auditor should consider whether the entity (1) can effectively identify and authenticate users, (2) has identified all of the access paths to the system and sensitive programs and data, and (3) has implemented techniques to effectively restrict access as intended. In evaluating the effectiveness of specific security techniques, the auditor should consider whether the software and/or hardware used has been independently tested and evaluated by organizations such as the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

To ensure that access controls are uniformly administered, the security management function should implement and maintain logical access controls based upon authorizations from appropriate levels within the entity.

A. Passwords, tokens, or other devices are used to identify and authenticate users

Identification is the process of distinguishing one user from all others, usually through the use of user IDs. User IDs are important because they are the means by which specific access privileges are assigned and recognized by the computer. However, the confidentiality of user IDs is typically not protected. For this reason, other means of authenticating users--that is, determining whether individuals are who they say they are--are typically implemented.

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

- Password selection is controlled by the assigned user.
- Passwords are changed periodically, about every 30 to 90 days. The more sensitive the data or the function, the more frequently passwords should be changed.
- Passwords are not displayed when they are entered.
- A minimum character length, at least 6 characters, is set for the passwords so that they cannot be easily guessed.
- Use of names, words, or old passwords within six generations is prohibited, while use of alphanumeric passwords should be encouraged since they are difficult to guess.
- Vendor-supplied passwords, such as SYSTEM, DEFAULT, USER, DEMO, and TEST, are replaced immediately upon implementation of a new system.
- Individual users are uniquely identified rather than having users within a group share the same ID or password.

To help ensure that passwords cannot be guessed, attempts to log on the system with invalid passwords should be limited. Typically, potential users are allowed three or four attempts to log on. This, in conjunction with the use of alphanumeric passwords, reduces the risk that an unauthorized user could gain access to a system by using a computer to try thousands of words or names until he or she found a password that provided access.

Another technique for reducing the risk of password disclosure is encrypting the password file. Although access to this file should be restricted to only a few people, encryption further reduces the risk that it could be accessed and read by unauthorized individuals.

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

A less common means of authentication is based on biometrics, an automated method of verifying or recognizing the identity of a person based on physiological or

behavioral characteristics. Biometrics devices include fingerprints, retina patterns, hand geometry, speech patterns, and keystroke dynamics. If auditors encounter such techniques, they should review the devices, observe the operations, and take whatever other steps may be necessary to evaluate their effectiveness, including obtaining the assistance of a specialist.

B. Identification of access paths

Users obtain access to data files and software programs through one or more access paths through the networks and computer hardware and software. Accordingly, to implement an appropriate level of security, it is important that the entity, to the extent possible, identify and control all access paths.

For stand-alone computers, identifying access paths may be a relatively simple task. However, in a networked environment careful analysis is needed to identify all of the system's entry points and paths to sensitive files. Networked systems typically consist of multiple personal computers that are connected to each other and to larger computers, such as file servers or mainframe processors. Many rely on public telephone networks and provide dial-in capabilities from virtually any remote location. As a result, the entry points to the system can be numerous. Also, once the system has been entered, the software programs available may provide multiple paths to various data resources and sensitive software programs.

Connecting to the Internet brings a multitude of vulnerabilities for an entity with potential access from millions of people from over 150 different countries. Incidents have shown that some Internet users are motivated to try and penetrate connected systems and have sophisticated software tools as aids, such as software to repeatedly attempt access using different passwords.

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

If entry points and access paths are not identified, they may not be adequately controlled and may be exploited by unauthorized users to bypass existing controls and gain access to sensitive data, programs, or password files. Further, managers will have an incomplete understanding of the risks associated with their systems and, therefore, may make erroneous risk management decisions. If all access paths cannot be identified, due to the complexity of the system and its connections to other systems, then managers should consider this unmeasurable risk in their risk management decisions.

C. Logical controls over data files and software programs

The most commonly used means of restricting access to data files and software programs is through the use of access control software, also referred to as security software. Access control software provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted. In addition, it provides a means of automatically logging and reporting access activity.

Although many types of software include security features designed to protect one application or one set of files, it is preferable to use access control software that secures the entire environment by protecting all of the applications available under one central operating system. Such software can be implemented in such a way that it complements the security features provided by more narrowly focused software controls. In this way the access control software can provide comprehensive and coordinated security. Examples of commonly used access control software packages that are capable of securing the entire operating system environment include RACF, ACF2, and Top Secret.

Generally, access control software provides many access control options that must be activated and tailored to the entity's needs in order to be effective. Examples of options that can be selected include

- what precise resources (data files and software) each user may access;
- what types of access authorized users are granted (e.g., read, update, delete, merge, execute);
- what days and what times of day a user may exercise specific privileges;
- password length and syntax (e.g., numeric or alphanumeric) and maximum life span;
- number of unsuccessful access attempts allowed;

- whether and after what period inactive IDs are revoked or terminals are logged off; and
- whether unauthorized access is actually prevented or if unauthorized access is allowed, but with a warning message to the user and/or the resource owner.

One of the auditor's primary tasks is to determine which options have been activated and whether they are in accordance with the access authorizations established by the resource owners.

Also, to protect against tampering with selected settings

- security profiles or tables should be protected from unauthorized access and modification either by restricting the paths to them or by encrypting them;
- access to the access control software itself should be restricted to authorized persons within the security function to minimize the risk of unauthorized changes being made to the settings;
- security profile override capabilities should be restricted to a few trusted individuals; and
- security access audit trails, which document use of the access control software, should be protected from unauthorized modification.

The entity's use of system standards or naming conventions for resources, such as data files, program libraries, individual programs, and applications, are important to this area and affect the efficiency of using access control software. For example, "pay" might identify all programs in a payroll application and the "100" series might be used for programs associated with inputting transactions for time and attendance and pay withholdings. Using this naming convention, access control software could restrict access to a limited number of payroll clerks who were authorized to enter the time and attendance and pay withholding information.

Appendix III to OMB Circular No. A-130 acknowledges that penetration testing can be a valuable tool when reviewing the security of a system. The suggested audit procedures for this section contain details on penetration testing that GAO has found useful in identifying security weaknesses. (See also section SS-1.2 for penetration analysis relevant to system software.)

D. Logical controls over a database

Logical controls may be implemented over an entire database through the use of database management system software (DBMS). This software can be used to control, organize, and manipulate data, provide multiple ways to access data in a database, and manage integrated data that cross operational, functional, and organizational boundaries within an organization. For example, personnel who have access to most of the information maintained in a personnel database may be restricted from viewing specific sensitive data fields, such as those containing salary data. Data dictionary software, which interfaces with DBMS and provides a method for documenting elements of a database, also may provide a method of securing data.

As with the logical controls over data files and software, the auditor's primary task is to determine if access settings have been implemented in accordance with the access authorizations established by the resource owners. Also, access to DBMS and data dictionary software and related tables should be protected from unauthorized changes through the use of logical access controls, encryption, and audit trails.

E. Logical controls over telecommunications access

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

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

- verify terminal identifications to restrict access through specific terminals;
- verify IDs and passwords for access to specific applications;
- control access between telecommunications systems and terminals;
- restrict an application's use of network facilities;
- automatically disconnect at the end of a session;

- provide network activity logs that can be used to monitor network use and configuration;
- allow authorized users to shut down network components;
- monitor dial-in access to the system by monitoring the source of calls or by disconnecting and then dialing back users at preauthorized phone numbers;
- restrict in-house access to communications software;
- control changes to communications software; and
- restrict and monitor access to telecommunications hardware or facilities.

As with other access controls, to be effective, telecommunications controls must be properly implemented in accordance with authorizations that have been granted. In addition, tables or lists used to define security limitations must be protected from unauthorized modification, and in-house access to communications security software must be protected from unauthorized access and modification.

In addition to technical controls, the initial screen viewed by an individual accessing an entity's systems through a telecommunications network should discourage unauthorized users from attempting access and make it clear that unauthorized browsing will not be tolerated. For example, an opening warning screen should state that the system is for authorized users only and that activity will be monitored. Also, dial-in phone numbers should not be published and should be periodically changed.

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

AC-3.3: Cryptographic tools

In some cases--especially those involving telecommunications--it is not possible or practical to adequately restrict access through either physical or logical access controls. In these cases, cryptographic tools can be used to identify and authenticate users and help protect the integrity and confidentiality of data and computer programs, both while these data and programs are "in" the computer system and while they are being transmitted to another computer system or stored on removable media, such as floppy disks, which may be held in a remote location.

Cryptography involves the use of algorithms (mathematical formulae) and combinations of keys (strings of bits) to do any or all of the following:

- Encrypt, or electronically scramble, a message or file so that it is unintelligible to those who do not have the secret key needed to decrypt it, thus keeping the contents of the message or file confidential.
- Provide an electronic signature that can be used to
  - determine if any changes have been made to the related file, thus ensuring the file's integrity, and
  - link a message or document to a specific individual's or group's key, thus ensuring that the "signer" of the file can be identified.

Cryptographic tools are especially valuable for any application that involves "paperless" transactions or for which the users want to avoid relying on paper documents to substantiate data integrity and validity. Examples include

- electronic commerce, where purchase orders, receiving reports, and invoices are created, approved, and transmitted electronically,
- travel administration, where travel orders and travel vouchers are created, approved, and transmitted electronically, and
- protection of documents or digital images, such as contracts, personnel records, or diagrams, that are stored on electronic media.

Cryptographic tools may be linked to an individual application or implemented so that they can be used to sign or encrypt data associated with multiple applications. For example, the personal computers connected to a local area network (LAN) may each be fitted with hardware and/or software that identifies and authenticates users and allows them to encrypt, sign, and authenticate the messages and files that they send or receive, regardless of the application that they are using.

There are a number of technical issues to consider concerning cryptography. Some of the key considerations are listed below.

- Are the cryptographic tools implemented in software or through the use of a hardware module? (Hardware modules are generally more secure.)
- How is the data transmitted between the computer's memory and the cryptographic module, and is this path protected?
- How strong, or complex, is the algorithm used to encrypt and sign data?
- How are keys managed and distributed?
- Does the entity's use of cryptographic tools comply with related Federal Information Processing Standards issued by NIST?
- Has the entity chosen cryptographic techniques that are appropriate to cost-effectively meet its defined control objectives?

The use of cryptography to protect sensitive data is increasing as the use of computer networks increases. However, its use is not yet widespread in federal non-classified systems and the related techniques are evolving. For these reasons, the discussion provided here is brief. If the auditor encounters cryptographic tools and determines that their reliability is important to his or her understanding of the controls, he or she should obtain the most recent guidance available from OMB, NIST, and GAO, as well as technical assistance from an auditor experienced is assessing cryptographic tools.

AC-3.4: Sanitation of equipment and media prior to disposal or reuse

The entity should have procedures in place to clear sensitive information and software from computers, disks, and other equipment or media when they are disposed of or transferred to another use. If sensitive information is not fully cleared, it may be recovered and inappropriately used or disclosed by individuals who have access to the discarded or transferred equipment and media.

The responsibility for clearing information should be clearly assigned. Also, standard forms or a log should be used to document that all discarded or transferred items are examined for sensitive information and that this information is cleared before the items are released.

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

Control Activities	Control Techniques	Audit Procedures
AC-3.1 Adequate physical security controls have been implemented.		*These audit procedures should be coordinated with section SC-.2.2 (environmental controls) since many of the control objectives and techniques are the same.*
A. Physical safeguards have been established that are commensurate with the risks of physical damage or access.	Facilities housing sensitive and critical resources have been identified. All significant threats to the physical well-being of sensitive and critical resources have been identified and related risks determined.	Review a diagram of the physical layout of the computer, telecommunications, and cooling system facilities. Walk through facilities. Review risk analysis.
	Access is limited to those individuals who routinely need access through the use of guards, identification badges, or entry devices, such as key cards. Management regularly reviews the list of persons with physical access to sensitive facilities.	Review lists of individuals authorized access to sensitive areas and determine the appropriateness for access. Before becoming recognized as the auditor, attempt to access sensitive areas without escort or identification badges. Observe entries to and exits from facilities during and after normal business hours. Observe utilities' access paths. Interview management.
	Keys or other access devices are needed to enter the computer room and tape/media library.	Observe entries to and exits from sensitive areas during and after normal business hours. Interview employees.
	All deposits and withdrawals of tapes and other storage media from the library are authorized and logged.	Review procedures for the removal and return of storage media from and to the library. Select from the log some returns and withdrawals, verify the physical existence of the tape or other media, and determine whether proper authorization was obtained for the movement.
	Unissued keys or other entry devices are secured.	Observe practices for safeguarding keys and other devices.

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

Control Activities	Control Techniques	Audit Procedures
A. Physical safeguards have been established that are commensurate with the risks of physical damage or access. (continued)	Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to reenter after fire drills, etc.	Review written emergency procedures. Examine documentation supporting prior fire drills. Observe a fire drill.
B. Visitors are controlled.	Visitors to sensitive areas, such as the main computer room and tape/media library, are formally signed in and escorted.	Review visitor entry logs. Observe entries to and exits from sensitive areas during and after normal business hours. Interview guards at facility entry.
	Entry codes are changed periodically.	Review documentation on and logs of entry code changes.
	Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.	Observe appointment and verification procedures for visitors.
AC-3.2 Adequate logical access controls have been implemented.		
A. Passwords, tokens, or other devices are used to identify and authenticate users.	Passwords are • unique for specific individuals, not groups; • controlled by the assigned user and not subject to disclosure; • changed periodically--every 30 to 90 days; • not displayed when entered; • at least 6 alphanumeric characters in length; and • prohibited from reuse for at least 6 generations.	Review pertinent policies and procedures. Interview users. Review security software password parameters. Observe users keying in passwords. Attempt to log on without a valid password; make repeated attempts to guess passwords. Assess procedures for generating and communicating passwords to users.
	Use of names or words is prohibited.	Review a system-generated list of current passwords. Search password file using audit software.
	Vendor-supplied passwords are replaced immediately.	Attempt to log on using common vendor-supplied passwords. Search password file using audit software.

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

Control Activities	Control Techniques	Audit Procedures
A. Passwords, tokens, or other devices are used to identify and authenticate users. (continued)	Generic user IDs and passwords are not used.	Interview users and security managers. Review a list of IDs and passwords.
	Attempts to log on with invalid passwords are limited to 3-4 attempts.	Repeatedly attempt to log on using invalid passwords. Review security logs.
	Personnel files are automatically matched with actual system users to remove terminated or transferred employees from the system.	Review pertinent policies and procedures. Review documentation of such comparisons. Interview security managers. Make comparison using audit software.
	Password files are encrypted.	View dump of password files (e.g., hexadecimal printout).
	For other devices, such as tokens or key cards, users • maintain possession of their individual tokens, cards, etc, and • understand that they must not loan or share these with others and must report lost items immediately.	Interview users. To evaluate biometrics or other technically sophisticated authentication techniques, the auditor should obtain the assistance of a specialist.
B. Identification of access paths.	An analysis of the logical access paths is performed whenever changes to the system are made.	Review access path diagram.
C. Logical controls over data files and software programs.	Security software is used to restrict access. Access to security software is restricted to security administrators only.	Interview security administrators and system users. Review security software parameters.
	Computer terminals are automatically logged off after a period of inactivity.	Observe terminals in use. Review security software parameters.
	Inactive users' accounts are monitored and removed when not needed.	Review security software parameters. Review a system-generated list of inactive logon IDs and determine why access for these users has not been terminated.

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

Control Activities	Control Techniques	Audit Procedures
C. Logical controls over data files and software programs. (continued)	Security administration personnel set parameters of security software to provide access as authorized and restrict access that has not been authorized. This includes access to data files, load libraries, batch operational procedures, source code libraries, security files, and operating system files. Naming conventions are used for resources.	Determine library names for sensitive or critical files and libraries and obtain security reports of related access rules. Using these reports, determine who has access to critical files and libraries and whether the access matches the level and type of access authorized. Perform penetration testing by attempting to access and browse computer resources including critical data files, production load libraries, batch operational procedures (e.g., JCL libraries), source code libraries, security software, and the operating system. These tests should be performed as (1) an "outsider" with no information about the entity's computer systems, (2) an "outsider" with prior knowledge about the systems--e.g., an ex-insider, and (3) an "insider" with and without specific information about the entity's computer systems and with access to the entity's facilities. When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet. When performing insider tests, use an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, try to access the entity's computer resources using default/generic IDs with easily guessed passwords. Determine whether naming conventions are used.

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

Control Activities	Control Techniques	Audit Procedures
D. Logical controls over a database.	Database management systems (DBMS) and data dictionary (DD) controls have been implemented that • restrict access to data files at the logical data view, field, or field-value level; • control access to the DD using security profiles and passwords; • maintain audit trails that allow monitoring of changes to the DD; and • provide inquiry and update capabilities from application program functions, interfacing DBMS, or DD facilities.	Review pertinent policies and procedures. Interview database administrator. Review DBMS and DD security parameters. Test controls by attempting access to restricted files.
	Use of DBMS utilities is limited.	Review security system parameters.
	Access and changes to DBMS software are controlled.	
	Access to security profiles in the DD and security tables in the DBMS is limited.	
E. Logical controls over telecommunications access.	Communication software has been implemented to • verify terminal identifications in order to restrict access through specific terminals; • verify IDs and passwords for access to specific applications; • control access through connections between systems and terminals; • restrict an application's use of network facilities; • protect sensitive data during transmission; • automatically disconnect at the end of a session; • maintain network activity logs; • restrict access to tables that define network options, resources, and operator profiles; • allow only authorized users to shut down network components; • monitor dial-in access by monitoring the source of calls or by disconnecting and then dialing back at preauthorized phone numbers; • restrict in-house access to telecommunications software; • control changes to telecommunications software; • ensure that data are not accessed or modified by an unauthorized user during transmission or while in temporary storage; and • restrict and monitor access to telecommunications hardware or facilities.	Review pertinent policies and procedures. Review parameters set by communications software or teleprocessing monitors. Test telecommunications controls by attempting to access various files through communications networks. Identify all dial-up lines through automatic dialer software routines and compare with known dial-up access. Discuss discrepancies with management. Interview telecommunications management staff and users.

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

Control Activities	Control Techniques	Audit Procedures
E. Logical controls over telecommunications access. (continued)	In addition to logical controls: The opening screen viewed by a user provides a warning and states that the system is for authorized use only and that activity will be monitored. Dial-in phone numbers are not published and are periodically changed.	Review pertinent policies and procedures. View the opening screen seen by telecommunication system users. Review documentation showing changes to dial-in numbers. Review entity's telephone directory to verify that the numbers are not listed.
AC-3.3 Cryptographic tools.	Cryptographic tools have been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs.	To evaluate cryptographic tools, the auditor should obtain the assistance of a specialist.
AC-3.4 Sanitation of equipment and media prior to disposal or reuse.	Procedures are implemented to clear sensitive data and software from discarded and transferred equipment and media.	Review written procedures. Interview personnel responsible for clearing equipment and media. For a selection of recently discarded or transferred items, examine documentation related to clearing of data and software. For selected items still in the entity's possession, test that they have been appropriately sanitized.

Critical Element AC-4: Monitor access, investigate apparent security violations, and take appropriate remedial action

As discussed under Critical Element AC-3, security software generally provides a means of determining the source of a transaction or an attempted transaction and of monitoring users' activities (the audit trail). However, to be effective (1) this feature should be activated to maintain critical audit trails and report unauthorized or unusual activity and (2) managers should review and take action on these reports.

AC-4.1: Audit trails are maintained

Access control software should be used to maintain an audit trail of security accesses to determine how, when, and by whom specific actions were taken. Such information is critical in monitoring compliance with security policies and when investigating security incidents.

The settings of the access control software controls the nature and extent of audit trail information that is provided. Typically, audit trails may include user ID, resource accessed, date, time, terminal location, and specific data modified. The completeness and value of the audit trails maintained will only be as good as the entity's ability to thoroughly identify the critical processes and the related information that may be needed.

Procedures for maintaining audit trails should be based on

- the value or sensitivity of data and other resources affected;
- the processing environment, e.g., system development, testing, or production;
- technical feasibility; and.
- legal and regulatory requirements.

AC-4.2: Actual or attempted unauthorized, unusual, or sensitive access is monitored

Because all of the audit trail information maintained is likely to be too voluminous to review on a routine basis, the security software should be implemented to selectively identify unauthorized, unusual, and sensitive access activity, such as

- attempted unauthorized access;
- access trends and deviations from those trends;
- access to sensitive data and resources;
- highly-sensitive privileged access, such as the ability to override security controls;
- access modifications made by security personnel; and
- unsuccessful attempts to log on to a system.

The security software should be designed to report such activity and, in some cases, respond by actions such as

- disabling passwords,
- terminating repeated failed attempts to access sensitive resources,
- terminating processing,
- shutting down terminals,
- issuing warning or error messages, and
- writing audit trail records that would not normally be maintained.

AC-4.3: Suspicious access activity is investigated and appropriate action taken

Once unauthorized, unusual, or sensitive access activity is identified, it should be reviewed and apparent or suspected violations should be investigated. If it is determined that a security violation has occurred, appropriate action should be taken to identify and remedy the control weaknesses that allowed the violation to occur, repair any damage that has been done, and determine and discipline the perpetrator. It is important that an entity have formal written procedures for reporting security violations or suspected violations to a central security management office so that multiple related incidents can be identified, others can be alerted to potential threats, and appropriate investigations can be performed. Such incidents might include multiple attacks by a common hacker or repeated "infections" with the same computer virus.

Without prompt and appropriate responses to security incidents, violations could continue to occur and cause damage to an entity's resources indefinitely. Further, violators will not be deterred from continuing inappropriate access activity, which could cause embarrassment to the entity and result in financial losses and disclosure of confidential information.

An entity should have documented procedures in place for responding to security violations. These should include procedures and criteria for

- documenting offenses,
- determining the seriousness of violations,
- reporting violations to higher levels of management,
- investigating violations,
- imposing disciplinary action for specific types of violations,
- notifying the resource owner of the violation, and
- reporting suspected criminal activity to law enforcement officials.

In addition, the frequency and magnitude of security violations and the corrective actions that have been taken should periodically be summarized and reported to senior management. Such a report can assist management in its overall management of risk by identifying the most attractive targets, trends in types of violations, cost of securing the entity's operations, and any need for additional controls.

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

Control Activities	Control Techniques	Audit Procedures
AC-4.1 Audit trails are maintained.	All activity involving access to and modifications of sensitive or critical files is logged.	Review security software settings to identify types of activity logged.
AC-4.2 Actual or attempted unauthorized, unusual, or sensitive access is monitored.	Security violations and activities, including failed logon attempts, other failed access attempts, and sensitive activity, are reported to management and investigated.	Review pertinent policies and procedures. Review security violation reports. Examine documentation showing reviews of questionable activities.

Control Techniques and Suggested Audit Procedures for Critical Element AC-4		
Control Activities	**Control Techniques**	**Audit Procedures**
AC-4.3 Suspicious access activity is investigated and appropriate action taken.	Security managers investigate security violations and report results to appropriate supervisory and management personnel. Appropriate disciplinary actions are taken.	Test a selection of security violations to verify that follow-up investigations were performed and to determine what actions were taken against the perpetrator.
	Violations are summarized and reported to senior management.	Interview senior management and personnel responsible for summarizing violations. Review any supporting documentation.
	Access control policies and techniques are modified when violations and related risk assessments indicate that such changes are appropriate.	Review policies and procedures and interview appropriate personnel. Review any supporting documentation.

Sources of Additional Information on Access Control

Information Systems Audit and Control Foundation, CobiT: Control Objectives for Information *and* Related Technology, 1998

NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, December 1996.

NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, December 1995.

Office of Technology Assessment, Issue Update on Information Security and Privacy in Network Environments, July 1995.

Office of Technology Assessment, Information Security and Privacy in Network Environments, September 1994.

Lainhart, and Donahue, The Information Systems Control Foundation, Computerized Information Systems (CIS) Audit Manual: A Guide to CIS Auditing in Government Organizations, July 1992.

Audit, Control, and Security of RACF (Technical Reference Series), Ernst & Young, 1992.

The Institute of Internal Auditors Research Foundation, Systems Auditability and Control: Module 9 - Security, April 1991.

Audit, Control, and Security of CA-ACF2 (Technical Reference Series), Ernst & Young, 1991.

Audit, Control, and Security of CA-TOP SECRET (Technical Reference Series), Ernst & Young, 1991.

[This page intentionally left blank.]

3.3 APPLICATION SOFTWARE DEVELOPMENT AND CHANGE CONTROL (CC)

Application software is designed to support a specific operation, such as payroll or loan accounting. Typically, several applications may operate under one set of operating system software. Controls over operating system software are discussed in Section 3.4.

Establishing controls over the modification of application software programs helps to ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled. Without proper controls, there is a risk that security features could be inadvertently or deliberately omitted or "turned off" or that processing irregularities or malicious code could be introduced. For example,

- a knowledgeable programmer could surreptitiously modify program code to provide a means of bypassing controls to gain access to sensitive data;
- the wrong version of a program could be implemented, thereby perpetuating outdated or erroneous processing that is assumed to have been updated; or
- a virus could be introduced, inadvertently or on purpose, that disrupts processing.

The primary focus of this section is on controlling the changes that are made to software systems in operation, since operational systems produce the financial statements and the majority of program changes are made to maintain operational systems. However, the same risks and mitigating controls apply to changes associated with systems under development, once their baseline requirements have been formally approved by both user management and the project development team.[1]

Assessing controls over application software development and modification involves evaluating the entity's success in performing each of the critical elements listed below.

---

[1]For reviews of systems under development or major system enhancements, auditors may want to consult GAO's System Assessment Framework: A Guide for Reviewing Information Management and Technology Issues in the Federal Government (GAO/AIMD-10.1.12, August 1996). This document provides more comprehensive guidance regarding system development issues and the phases associated with a System Development Life Cycle (SDLC) methodology.

Critical Elements

CC-1 Processing features and program modifications are properly authorized

CC-2 Test and approve all new and revised software

CC-3 Control software libraries

Critical Element CC-1: Processing features and program modifications are properly authorized

The processing features built into application software should be authorized by the managers responsible for the agency program or operations that the application supports. This is because these are the managers responsible for seeing that software supporting their operations meets their needs and produces reliable data and that the operations are carried out in accordance with applicable laws, regulations, and management policies. For example, the processing features associated with loan accounting software should be authorized by the loan program managers. Such user or owner authorization is needed when new systems are being developed, as well as when operational systems are being modified.

Authorization is the first step in implementing the features or the changes that have been decided on by the users, and the entity should have a process for obtaining, documenting, and communicating such authorizations as part of its system development life cycle (SDLC) methodology. If authorization procedures have not been developed or are not followed, an individual might be able to initiate program changes that result in erroneous processing or weakened access controls or edits built into the software.

A related issue is the entity's policies regarding employee's use of public domain software or personal software. Concerns regarding such software include the increased risk that viruses will be introduced, errors in the software will lead to bad decisions, and copyright laws may be violated.

CC-1.1: A System Development Life Cycle Methodology has been implemented

The entity should have a documented SDLC methodology that details the procedures that are to be followed when applications are being designed and developed, as well as when they are subsequently modified. The SDLC should provide a structured approach for identifying and documenting needed changes to computerized operations; assessing the costs and benefits of various options, including the feasibility of using off-the-shelf software; and designing, developing, testing, and approving new systems and system modifications. Especially for new systems being developed or for major enhancements to existing systems, it is important that SDLC require approving design features at key points during the design and development process.

For the methodology to be properly applied, it should be sufficiently documented to provide staff with clear and consistent guidance. Also, personnel involved in designing, developing, and implementing new systems and system modifications should be appropriately trained. This includes program staff who initiate requests for modifications and staff involved in designing, programming, testing, and approving changes.

More detailed information on assessing system development efforts is available in GAO's System Assessment Framework document (GAO/AIMD-10.1.12).

CC-1.2: Authorizations for software modifications are documented and maintained

Policies and procedures should be in place that detail who can authorize a modification and how these authorizations are to be documented. Generally, the application users have the primary responsibility for authorizing systems changes. However, users should be required to discuss their proposed changes with systems developers to confirm that the change is feasible and cost effective. For this reason, an entity may require a senior systems developer to co-authorize a change.

The use of standardized change request forms helps ensure that requests are clearly communicated and that approvals are documented. Authorization documentation should be maintained for at least as long as a system is in operation in case questions arise regarding why or when system modifications were made. Authorization documents may be maintained in either paper or electronic form as long as their integrity is protected.

CC-1.3: Use of public domain and personal software is restricted

It is important that an entity have clear policies regarding the use of personal and public domain software by employees at work. Allowing employees to use their own software, or even use diskettes for data storage that have been used elsewhere, increases the risk of introducing viruses. It also increases the risk of violating copyright laws and making bad decisions based on incorrect information produced by erroneous software. As mentioned is section SP-3.4, virus identification software can help contain damage from viruses, which may be introduced from unauthorized use of public domain or personal software or from corrupted diskettes.

Control Techniques and Suggested Audit Procedures for Critical Element CC-1		
Control Activities	**Control Techniques**	**Audit Procedures**
CC-1.1 A system development life cycle methodology (SDLC) has been implemented.	A SDLC methodology has been developed that • provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process, • is sufficiently documented to provide guidance to staff with varying levels of skill and experience, • provides a means of controlling changes in requirements that occur over the system's life, and • includes documentation requirements.	Review SDLC methodology. Review system documentation to verify that SDLC methodology was followed.
	Program staff and staff involved in developing and testing software have been trained and are familiar with the use of the organization's SDLC methodology.	Interview staff. Review training records.
CC-1.2 Authorizations for software modifications are documented and maintained.	Software change request forms are used to document requests and related approvals. Change requests must be approved by both system users and data processing staff.	Identify recent software modifications and determine whether change request forms were used. Examine a selection of software change request forms for approvals. Interview software development staff.
CC-1.3 Use of public domain and personal software is restricted.	Clear policies restricting the use of personal and public domain software have been developed and are enforced. The entity uses virus identification software.	Review pertinent policies and procedures. Interview users and data processing staff.

Critical Element CC-2: Test and approve all new and revised software

A disciplined process for testing and approving new and modified programs prior to their implementation is essential to make sure programs operate as intended and that no unauthorized changes are introduced. The extent of testing varies depending on the type of modification. For new systems being developed or major system enhancements, testing will be extensive, generally progressing through a series of test stages that include (1) testing individual program modules (unit testing), (2) testing groups of modules that must work together (integration testing), and (3) testing an entire system (system testing). Minor modifications may require less extensive testing; however, changes should still be carefully controlled and approved since relatively minor program code changes, if done incorrectly, can have a significant impact on overall data reliability.

CC-2.1: Changes are controlled as programs progress through testing to final approval

Once a change has been authorized, it should be written into the program code and tested in a disciplined manner. Because testing is an iterative process that is generally performed at several levels, it is important that the entity adhere to a formal set of procedures or standards for prioritizing, scheduling, testing, and approving changes. These procedures should be described in the entity's SDLC and should include requirements for

- ranking and scheduling changes so that authorized change requests are not lost and are implemented efficiently and in accordance with user needs;
- preparing detailed specifications for the program change, which are approved by an individual responsible for supervising programming activities to confirm that the specifications correspond to the user's authorized requirements;
- developing a detailed test plan for each modification that defines the levels and types of tests to be performed;
- defining responsibilities for each person involved in testing and approving software (e.g., systems analysts, programmers, quality assurance staff, auditors, library control personnel, and users--who should participate in testing and approve test results prior to implementation);
- developing related changes to system documentation, including hardware documentation, operating procedures, and user procedures;
- supervisory review and documented approvals by appropriate personnel, including programming supervisors, database administrators, and other technical personnel prior to and after testing;

- maintaining controlled libraries of software in different stages of development to ensure that programs being developed or tested are not interchanged with each other or with production software (controls associated with software libraries are discussed further in this section under critical element CC-3);
- documenting changes so that they can be traced from authorization to the final approved code and facilitating "trace-back" of code to design specifications and functional requirements by system testers; and
- obtaining final user acceptance only after testing is successfully completed and reviewed by the user.

When testing at any stage of the process shows the need for additional software modifications, these modifications should also be tested. A large number of unsuccessful tests, such as tests that lead to unexpected processing terminations, referred to as abnormal endings (abends), may indicate that coding was incorrectly performed and that earlier testing was not adequate or not adequately controlled. Also, a high number of abends with implemented systems may indicate inadequate testing prior to implementation.

To be effective, tests should be conducted in an environment that simulates the conditions that are likely to be encountered when the new or modified software is implemented. To do this, a set of test transactions and data should be developed that contains examples of the various types of situations and information that the newly designed program will have to handle, including invalid transactions or conditions to make certain the new software recognizes these transactions and reacts appropriately. In addition, the system's ability to process the anticipated volume of transactions within expected time frames should be tested.

Test transactions and data can be developed based on actual transactions and data. However, steps should be taken to ensure that current "live" data are not impaired. Live data and transactions should not be used in testing unless both an existing system and a test system are operating simultaneously and the live data are used to build test data files. When such parallel processing is used, care should be taken to clearly identify the data processed or maintained on the existing system as the "official" record of activity. However, live data testing needs to be supplemented with invalid transaction testing to determine whether invalid transactions are appropriately rejected. Testing through parallel processing allows continued operations with the old system until the modified system is determined to be effective.

All test data, transactions, and results should be saved and documented. This will facilitate future testing of other modifications and allow a reconstruction if future events necessitate a revisit of the actual tests and results.

CC-2.2. Emergency changes are promptly tested and approved

It is not uncommon for program changes to be needed on an emergency basis to keep a system operating. Some applications, such as payroll processing, are performed in cycles that must be completed by a deadline. Other systems must be continuously available so that the operations they support are not interrupted. In these cases, the risk of missing a deadline or disrupting operations may pose a greater risk than that of temporarily suspending program change controls. However, because of the increased risk that errors or other unauthorized modifications could be implemented, emergency changes should be kept to a minimum.

It is important that an entity follow established procedures to perform emergency software changes and reduce the risk of suspending or abbreviating normal controls. Generally, emergency procedures should specify

- when emergency software changes are warranted,
- who may authorize emergency changes,
- how emergency changes are to be documented, and
- within what period after implementation the change must be tested and approved.

Making emergency changes often involves using sensitive system utilities or access methods that grant much broader access than would normally be needed. In some cases, an emergency password or token providing needed access may be stored in a sealed envelope for use by programmers in an emergency. It is important that access to such devices be controlled and that their use be promptly reviewed. Control over the use of system utilities is discussed further in Section 3.4 on system software.

Shortly after an emergency change is made, the usual change controls should be applied retroactively. That is, the change should be subjected to the same review, testing, and approval process that applies to scheduled changes. In addition, logs of emergency changes and related documentation should be periodically reviewed by data center management or security administrators to determine whether all such changes have been tested and received final approval.

CC-2.3 Distribution and implementation of new or revised software is controlled

Many federal agencies have data processing operations that involve multiple locations and require a coordinated effort for effective and controlled distribution and implementation of new or revised software. For example, an agency may have a central software design, development, and maintenance activity, but have two or more regional data processing centers running the same software. Once a modified

software program has been approved for use, the change should be communicated to all affected parties and distributed and implemented in a way that leaves no doubt about when it is to begin affecting processing. To accomplish these objectives, an entity should have and follow established procedures for announcing approved changes and their implementation dates and for making the revised software available to those who need to begin using it.

Source code programs (the code created by programmers) are compiled into object or production code programs that are machine-readable and become the versions that are actually used during data processing. Source code programs should be closely controlled at a central location and compiled into production programs before being distributed. Source code should not be distributed to other locations. This helps protect the source code from unauthorized changes and increases the integrity of the object or production code, which is much more difficult for programmers to change without access to the source code. Inadequately controlling software distribution and implementation increases the risk that data could be improperly processed due to

- implementation of unapproved possibly malicious software,
- continued use of outdated versions of software, and
- inconsistent implementation dates resulting in inconsistent processing of similar data at different locations.

With independent processing sites, each site is responsible for implementing the correct version of the software at the predetermined date and time and maintaining the documentation authorizing such implementation. Conversely, implementing new software through one or more central computers or servers minimizes the risk that the software will be inconsistently implemented.

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

Control Activities	Control Techniques	Audit Procedures
CC-2.1 Changes are controlled as programs progress through testing to final approval.	Test plan standards have been developed for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, library control).	Review test plan standards.
	Detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.	For the software change requests selected for control activity CC-1.2: • review specifications; • trace changes from code to design specifications; • review test plans; • compare test documentation with related test plans; • analyze test failures to determine if they indicate ineffective software testing; • review test transactions and data; • review test results; • review documentation of management or security administrator reviews; • verify user acceptance; and • review updated documentation. Determine whether operational systems experience a high number of abends and, if so, whether they indicate inadequate testing prior to implementation.
	Software changes are documented so that they can be traced from authorization to the final approved code and they facilitate "trace-back" of code to design specifications and functional requirements by system testers.	
	Test plans are documented and approved that define responsibilities for each party involved (e.g., users, systems analysts, programmers, auditors, quality assurance, library control).	
	Unit, integration, and system testing are performed and approved • in accordance with the test plan and • applying a sufficient range of valid and invalid conditions.	
	A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing. Live data are not used in testing of program changes except to build test data files.	
	Test results are reviewed and documented.	
	Program changes are moved into production only upon documented approval from users and system development management.	
	Documentation is updated for software, hardware, operating personnel, and system users when a new or modified system is implemented.	
	Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.	

Control Techniques and Suggested Audit Procedures for Critical Element CC-2		
CC-2.2 Emergency changes are promptly tested and approved.	Emergency change procedures are documented.	Review procedures.
	Emergency changes are documented and • approved by the operations supervisor, • formally reported to computer operations management for follow-up, and • approved after the fact by programming supervisors and user management.	For a selection of emergency changes recorded in the emergency change log, review related documentation and approval.
CC-2.3 Distribution and implementation of new or revised software is controlled.	Standardized procedures are used to distribute new software for implementation.	Examine procedures for distributing new software.
	Implementation orders, including effective date, are provided to all locations where they are maintained on file.	Examine implementation orders for a sample of changes.

Critical Element CC-3: Control software libraries

To ensure that approved software programs are protected from unauthorized changes or impairment and that different versions are not misidentified, copies should be maintained in carefully controlled libraries. Further, adequately controlled software libraries help ensure that there is (1) a copy of the "official" approved version of a program available in case the integrity of an installed version is called into question and (2) a permanent historical record of old program versions.

Separate libraries should be established for programs being developed or modified, programs being tested by users, and programs approved for use (production programs). Access to these libraries should be limited and movement of programs and data among them should be controlled.

Inadequately controlled software libraries increase the risk that unauthorized changes could be made either inadvertently or deliberately for fraudulent or malicious purposes. In addition, inadequate controls over programs being developed or modified could make it difficult to determine which version of the program is the most recent. Such an environment can result in inefficiencies and could lead to monetary losses and interruptions of service. For example,

- an unauthorized program could be substituted for the authorized version;
- test programs could be labeled as production programs;
- two programmers could inadvertently access and work on the same test program version simultaneously, making it difficult or impossible to merge their work; or
- unauthorized changes to either test or production programs could be made surreptitiously and remain undetected.

CC-3.1 Programs are labeled and inventoried

Copies of software programs should be maintained in libraries where they are labeled, dated, inventoried, and organized in a way that diminishes the risk that programs will be misidentified or lost. Library management software provides an automated means of inventorying software, ensuring that differing versions are not accidentally misidentified, and maintaining a record of software changes. Specifically, such software can be used to

- produce audit trails of program changes and to maintain version number control,
- record and report program changes made,
- automatically number program versions,
- identify creation date information,
- maintain copies of previous versions, and
- control concurrent updates so that multiple programmers are prevented from making changes to the same program in an uncontrolled manner.

CC-3.2 Access to program libraries is restricted

Access to software libraries should be protected by the use of access control software or operating system features and physical access controls. Separate libraries should be established for (1) program development and maintenance, (2) user testing, and (3) production. Also, controlled copies of the source versions of all programs (the code created by programmers) should be separately maintained and protected from unauthorized access. If unauthorized modifications are suspected of a production program, the source code can be recompiled to determine what has been changed. Only the library control group should be allowed to compile source code and, thus, create production programs.

CC-3.3 Movement of programs and data among libraries is controlled

The movement of programs and data among libraries should be controlled by an organization segment that is independent of both the user and the programming staff. This group should be responsible for

- moving programs from development/maintenance to user testing and from user testing to production;
- supplying data from the production library for testing and creating test data; and
- controlling different program versions, especially when more than one change is being performed on a program concurrently.

Prior to transferring a tested program from the user test library to the production library, the independent library control group should (1) generate a report that shows all changed source code (lines added, changed, and deleted) and (2) compare this report to the user request to ensure that only approved changes were made.

Control Techniques and Audit Procedures for Critical Element CC-3

Control Activities	Control Techniques	Audit Procedures
CC-3.1 Programs are labeled and inventoried.	Library management software is used to • produce audit trails of program changes, • maintain program version numbers, • record and report program changes, • maintain creation/date information for production modules, • maintain copies of previous versions, and • control concurrent updates.	Review pertinent policies and procedures. Interview personnel responsible for library control. Examine a selection of programs maintained in the library and assess compliance with prescribed procedures. Determine how many prior versions of software modules are maintained.
CC-3.2 Access to program libraries is restricted.	Separate libraries are maintained for program development and maintenance, testing, and production programs.	Examine libraries in use. Interview library control personnel.
	Source code is maintained in a separate library.	Examine libraries in use. Verify that source code exists for a selection of production load modules by (1) comparing compile dates, (2) recompiling the source modules, and (3) comparing the resulting module size to production load module size.
	Access to all programs, including production code, source code, and extra program copies, are protected by access control software and operating system features.	For critical software production programs, determine whether access control software rules are clearly defined. Test access to program libraries by examining security system parameters.
	All deposits and withdrawals of program tapes to/from the tape library are authorized and logged.	Select some program tapes from the log and verify the existence of the tapes either in the library or with the individual responsible for withdrawing the tapes.
CC-3.3 Movement of programs and data among libraries is controlled.	A group independent of the user and programmers controls movement of programs and data among libraries. Before and after images of program code are maintained and compared to ensure that only approved changes are made.	Review pertinent policies and procedures. For a selection of program changes, examine related documentation to verify that • procedures for authorizing movement among libraries were followed and • before and after images were compared.

Sources of Additional Information on Software Change Control

Information Systems Audit and Control Foundation, CobiT: Control Objectives for Information *and* Related Technology, 1998.

Lainhart and Donahue, The Information Systems Control Foundation, Computerized Information Systems (CIS) Audit Manual: A Guide to CIS Auditing in Government Organizations, July 1992.

The Institute of Internal Auditors Research Foundation, Systems Auditability and Control: Module 5 - Managing Information and Developing Systems, April 1991.

Ruthberg, Fisher, and Lainhart, System Development Auditor, Elsevier Advanced Technology, 1991.

NIST Special Publication 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach, April 1988.

FIPS 132, Software Verification and Validation Plans, November 19, 1987.

FIPS 105, Software Documentation Management, June 6, 1984.

FIPS 102, Computer Security Certification and Accreditation, September 27, 1983.

FIPS 101, Lifecycle Validation, Verification and Testing of Computer Software, June 6, 1983.

[This page intentionally left blank.]

3.4 SYSTEM SOFTWARE (SS)

System software is a set of programs designed to operate and control the processing activities of computer equipment. Generally, one set of system software is used to support and control a variety of applications that may run on the same computer hardware. System software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on a system. Some system software can change data and program code on files without leaving an audit trail. The following are examples of system software:

- operating system software,
- system utilities,
- program library systems,
- file maintenance software,
- security software,
- data communications systems, and
- database management systems.

Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. Inadequate controls in this area could lead to unauthorized individuals using system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs; authorized users of the system gaining unauthorized privileges to conduct unauthorized actions; and/or systems software being used to circumvent edits and other controls built into application programs. Such weaknesses seriously diminish the reliability of information produced by all of the applications supported by the computer system and increase the risk of fraud and sabotage. System software programmers are often more technically qualified than other data processing personnel and, thus, have a greater ability to perform unauthorized actions if controls in this area are weak.

The control concerns for system software are similar to the access control issues discussed in section 3.2 and the software change control issues discussed in section 3.3. However, because of the high level of risk associated with system software activities, most entities have a separate set of control procedures that apply to them. For this reason, auditors generally treat this segment of the computer-related controls review separately.

Evaluating the adequacy of system software controls involves assessing the entity's efforts to perform each of the critical elements listed below.

Critical Elements

SS-1 Limit access to system software

SS-2 Monitor access to and use of system software

SS-3 Control system software changes

Critical Element SS-1: Limit access to system software

Restricting access to the different components of system software and related documentation is critical to controlling the overall integrity of information systems. If system software is not adequately protected, an individual could gain access to capabilities that would allow him or her to bypass security features found in either operating system security software or access controls built into application software. The individual would then be able to read, modify, or destroy application programs, master data files, and transaction data and subsequently erase any electronic audit trail of his or her activities.

In general, access control is needed for all components of systems software, including system utilities, program library systems, file maintenance systems, security software, data communications systems, and database management systems. Without proper control, damage could occur to individual components and some components could be used to access other components.

SS-1.1: Access authorizations are appropriately limited

Access to system software should be restricted to a very limited number of personnel whose job responsibilities require that they have such access. Typically, access to operating system software is restricted to a few systems programmers whose job it is to modify the system, when needed, and intervene when the system will not operate properly. In addition, database administrators need access to the system's database management system and a designated senior-level security administrator needs access to security software. However, application programmers and computer operators should not have access to system software as this would be incompatible with their assigned responsibilities and could allow unauthorized actions to occur. (See section 3.5 for details on segregation of duties.)

The number of personnel authorized to access the system will vary depending on the size and needs of the organization and, therefore, should be determined based on an analysis of the entity's operations. For example, a large organization that must maintain operations on a 24-hour basis will need more operating system analysts and programmers than a smaller organization that operates on a less intensive schedule.

There may be a tendency for entities to authorize access to many individuals so that emergency operating problems can be handled promptly. However, management must balance the need for efficiency with the need for security.

SS-1.2: All access paths have been identified and controls implemented to prevent or detect access for all paths

In order to control access, it is essential to analyze the system software configuration to identify all paths through which access to sensitive capabilities can be obtained. By identifying such paths, management can establish access controls to limit access to these paths and to facilitate monitoring of their use. If paths exist but are not identified, they may be exploited without detection.

In analyzing a system's configuration, it is important to consider the following.

- System interfaces--The various components of system software and application systems should interface in a manner that protects system integrity and does not allow security features to be bypassed or circumvented. Also, system software may be customized to alter processing through the use of exits. This customization allows for the insertion of programs or code to perform additional functions. However, if not properly authorized and controlled, the customized software can increase a system's vulnerability to unauthorized access by creating new paths to the system software or by executing unauthorized routines that could be used for malicious purposes.

- Vendor access packages--It is common for vendors to embed in the system software a capability that allows them to access the system. This capability makes it easier for the vendor to assist in resolving system operating problems. However, as with all access paths, this provides another means for knowledgeable unauthorized users to access the system.

- Vendor supplied default logon IDs and passwords--Computer system vendors supply default user IDs and passwords so that users can initially log on to a new system. Once users have established their own IDs and passwords, the vendor IDs and passwords should be deleted so that they cannot be used by unauthorized individuals. Users may not take this step due to either neglect or because they find it convenient to have an easy method of accessing the system. However, not deleting the vendor's IDs and passwords leaves the system extremely vulnerable to unauthorized access and severely diminishes the value of passwords as an access control.

- Remote access to the system master console--It may be possible to access the system software remotely through a network or through dialing in. All such access points should be identified and appropriately controlled.

As with the access controls discussed in section 3.2, access to sensitive system software can be controlled through logical and physical access controls. In addition, cryptography can be used to encrypt passwords so that they cannot be read.

Software tools are available to aid the auditor in analyzing the system software configuration. For example, a commercial package, CA-EXAMINE, is a tool to test the integrity of a specific vendor's operating system. Details on using this and similar tools are beyond the scope of this manual. However, the auditor should consult specific audit guides for the operating system being evaluated and should be experienced in using the specific software tool or seek the assistance of someone who is. Audited entities may own certain software tools and the auditor may want to consider requesting authorization from the entity to use an entity-owned tool during the audit. The suggested audit procedures for this section contain details on penetration analysis that GAO has found valuable in identifying security weaknesses. (See section AC-3.2 for penetration testing relevant to logical access controls.)

Control Techniques and Suggested Audit Procedures Critical Element SS-1

Control Activities	Control Techniques	Audit Procedures
SS-1.1 Access authorizations are appropriately limited.	Policies and procedures for restricting access to systems software exist and are up-to-date.	Review pertinent policies and procedures. Interview management and systems personnel regarding access restrictions.
	Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. Application programmers and computer operators are specifically prohibited from accessing system software.	Observe personnel accessing system software, such as sensitive utilities, and note the controls encountered to gain access. Attempt to access the operating system and other system software.
	Documentation showing justification and management approval for access to system software is kept on file.	Select some systems programmers and determine whether management-approved documentation supports their access to system software. Select some application programmers and determine whether they are not authorized access.
	The access capabilities of systems programmers are periodically reviewed for propriety to see that access permissions correspond with job duties.	Determine the last time the access capabilities of systems programmers were reviewed.

Control Techniques and Suggested Audit Procedures Critical Element SS-1		
Control Activities	**Control Techniques**	**Audit Procedures**
SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths.	The operating system is configured to prevent circumvention of the security software and application controls.	Test the operating system parameters to verify that it is configured to maintain the integrity of the security software and application controls. (The specifics of this step will be determined by the operating system in use. The auditor should consult audit guides for the operating system in use. This step may be facilitated by use of CA-EXAMINE, the DEC VAX Toolkit, or other audit tools. However, the auditor should be experienced in using the specific software tool, or seek the assistance of someone who is.)
		Obtain a list of vendor-supplied software and determine if any of these products have known deficiencies that adversely impact the operating system integrity controls. Judgmentally review the installation of system software components and determine whether they were appropriately installed to preclude adversely impacting operating system integrity controls.

Control Techniques and Suggested Audit Procedures Critical Element SS-1

Control Activities	Control Techniques	Audit Procedures
SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths. (continued)	The operating system is configured to prevent circumvention of the security software and application controls. (continued)	Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods including: •Determine whether the operating system's subsystems have been appropriately implemented to ensure that they support integrity controls. (For example, with MVS, the auditor should evaluate IPL controls; APF update controls and implementation of key MVS libraries and locally defined and tailored system libraries; SVC controls, including imbedded passwords and controls to prevent interception; SMF options; and PPT.) •Determine whether applications interfaces have been implemented to support operating system integrity controls, including on-line transaction monitors; database software; on-line editors; on-line direct-access storage devices; on-line operating system datasets; exits related to the operating system, security, and program products; and controls over batch processing, to include security controls, scheduler controls, and access authorities. (For example, with MVS, the evaluated interfaces should include CICS, ADABAS, IMS, IDMS, TSO and/or similar packages; on-line DASD volumes; and on-line MVS datasets, such as CLIST, PARMLIB, SPOOL, DUMP, and TRACE, I/O appendages, and JES2/JES3.) •Evaluate the controls over external access to computer resources including networks, dial-up, LAN, WAN, RJE, and the Internet. •Identify potential opportunities to adversely impact the operating system and its products through trojan horses, viruses, and other malicious actions.

Control Techniques and Suggested Audit Procedures Critical Element SS-1

Control Activities	Control Techniques	Audit Procedures
SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths. (continued)	Access to system software is restricted to personnel with corresponding job responsibilities by access control software. Update access should generally be limited to primary and backup systems programmers. All accesses to system software files are logged by automated logging facilities.	Obtain a list of all system software on test and production libraries used by the entity. Verify that access control software restricts access to system software. Using security software reports, determine who has access to system software files, security software, and logging files. Preferably, reports should be generated by the auditor, but at a minimum, they should be generated in the presence of the auditor. Verify that system programmer's access to production data and programs is only allowed under controlled updates and during emergencies when established procedures are followed.
	Vendor-supplied default logon IDs and passwords have been disabled.	Inquire whether disabling has occurred. Test for default presence using vendor standard IDs and passwords.
	Remote access to the system master console is restricted. Physical and logical controls provide security over all terminals that are set up as master consoles.	Determine what terminals are set up as master consoles and what controls exist over them. Test to determine if the master console can be accessed or if other terminals can used to mimic the master console and take control of the system.

Critical Element SS-2: Monitor access to and use of system software

Because of the powerful capabilities at the disposal of those who have access to system software, its use should be monitored to identify any inappropriate or unusual behavior. Such behavior may indicate unauthorized access or that an individual is improperly exploiting his or her access privileges. For example, greater than normal use of system software or use at odd hours may indicate that an individual is using the software to search for system weaknesses to exploit or to make unauthorized changes to system or application software or data.

For monitoring to be effective in both detecting and deterring inappropriate use, those authorized to use system software should understand (1) which uses are appropriate and which are not and (2) that their activities may be monitored. Such policies should be documented and distributed to all personnel.

SS-2.1: Policies and techniques have been implemented for using and monitoring use of system utilities

Some system utilities are used to perform system maintenance routines that are frequently required during normal processing operations. Other utilities aid the development and documentation of application systems. These utilities can aid individuals with fraudulent or malicious intentions in understanding the programs or data in an application system and how they operate or in making unauthorized modifications. For example, the following lists some utilities with their intended functions that could be misused without proper monitoring and control.

- Flowcharters, transaction profile analyzers, execution path analyzers, and data dictionaries can be used to understand application systems.
- Data manipulation utilities, data comparison utilities, and query facilities can be used to access and view data, with manipulation utilities also allowing data modifications.
- On-line debugging facilities permit on-line changes to program object code leaving no audit trail and can activate programs at selected start points.
- Library copiers can copy source code from a library into a program, text and on-line editors permit modification of program source code, and on-line coding facilities permit programs to be coded and compiled in an interactive mode.

To prevent or detect the misuse of system utilities, policies should be clearly documented regarding their use. In addition, the use of utilities should be monitored. Generally, systems software contains a feature that provides for logging and reporting the use of system software. Such reports should identify when and by whom the software was used. It is important that this function is working properly and that the reports are reviewed on a regular basis.

The availability of standard usage data may assist the systems manager in identifying unusual activity. Some systems can be designed to compare standard usage data with actual use and report significant variances, thus making it easier for the system manager to identify unusual activity.

SS-2.2: Inappropriate or unusual activity is investigated and appropriate actions taken

When questionable activity is identified, it should be investigated. If improper activity is determined to have occurred, in accordance with security violation policies (discussed in section 3.2), the incident(s) should be documented, appropriate disciplinary action should be taken, and higher level management notified. Further, the possibility of damage or alteration to the system software, application software, and related data files should be investigated and needed corrective actions taken. Such actions should include notifying the resource owner of the violation.

Control Techniques and Suggested Audit Procedures Critical Element SS-2

Control Activities	Control Techniques	Audit Procedures
SS-2.1 Policies and techniques have been implemented for using and monitoring use of system utilities.	Policies and procedures for using and monitoring use of system software utilities exist and are up-to-date.	Review pertinent policies and procedures. Interview management and systems personnel regarding their responsibilities.
	Responsibilities for using sensitive system utilities have been clearly defined and are understood by systems programmers.	
	Responsibilities for monitoring use are defined and understood by technical management.	
	The use of sensitive system utilities is logged using access control software reports or job accounting data (e.g., IBM's System Management Facility).	Determine whether logging occurs and what information is logged. Review logs. Using security software reports, determine who can access the logging files.
SS-2.2 Inappropriate or unusual activity is investigated and appropriate actions taken.	The use of privileged system software and utilities is reviewed by technical management.	Interview technical management regarding their reviews of privileged system software and utilities usage. Review documentation supporting their reviews.
	Inappropriate or unusual activity in using utilities is investigated.	Interview management and systems personnel regarding these investigations. Review documentation supporting these investigations.
	Systems programmers' activities are monitored and reviewed.	Interview systems programmer supervisors to determine their activities related to supervising and monitoring their staff. Review documentation supporting their supervising and monitoring of systems programmers' activities.
	Management reviews are performed to determine that control techniques for monitoring use of sensitive system software are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).	Interview management and analyze their reviews concerning the use of system software. Determine what management reviews have been conducted, and their currency, over this area.

Critical Element SS-3: Control system software changes

Modifications to system software should be controlled so that only authorized and properly tested changes are implemented. If system software is not adequately controlled and tested, system parameters may be inadequate to prevent unauthorized changes to application programs or data. Furthermore, software malfunctions during processing runs could result in inaccurate or incomplete financial data. Controls should provide that all changes are tested and approved and that only approved system software is implemented.

SS-3.1: System software changes are authorized, tested, and approved before implementation

The entity should have a standard procedure for identifying, selecting, installing, and modifying system software to meet its operational needs. The procedure should include an analysis of costs and benefits associated with the system software and specific consideration of the software's impact on processing reliability and security.

System software changes may be needed to correct identified problems, to install a vendor's latest system software version, or to enhance operational efficiencies. All changes should be made under a controlled environment to protect system software integrity. Procedures should exist to identify and document system software problems along with their related analysis and resolution. Specifically, systems software problems should be recorded in a log that identifies the problem, the individual assigned to analyze the problem, and how the problem was resolved. All changes should be supported with a request for change document that includes a stated purpose for the change and an authorization to make the change.

A written standard should exist for testing changes to existing system software and new versions and products that serves as a guide to systems programmers and their managers. Testing should be done in a test environment and not in the production environment. Testing should include checking the logic of the system software to be changed as well as how it works in conjunction with other software on the system. Testing results should be documented and the results reviewed by technically qualified subject area experts who document their opinions that the system software is ready for production use. Data center management should review the testing results and documentation prior to granting approval to move the system software into production use.

Some system software includes security-related features that are optional and can be turned off or on by the systems programmer. Features desired should be specified, and the testing and review process should verify that the features are turned on.

On occasion, emergency changes may be required directly to production programs. These should be documented and authorized at the time and should be reported and reviewed by an independent supervisor in the IS department. (Section 3.3, Software Change Control, discusses controls needed over application systems. Concerns over system software changes are similar.)

SS-3.2: Installation of system software is documented and reviewed

When possible, the installation of system software changes and new versions or products should be scheduled to minimize the impact on data processing operations, and an advance notice should be provided to system software users. The actual installation should be logged to establish an audit trail and reviewed by data center management. The migration of system software from the testing environment to the production environment should be done, after approval, by an independent library control group. Outdated versions of system software should be removed from the production environment to preclude their future use. Some changes may be made specifically to correct security or integrity vulnerabilities, and using outdated versions allows the entity's data and systems to remain exposed to these vulnerabilities.

All vendor-supplied system software should be supported by the vendor. Vendors often release new versions of system software products and may discontinue support of earlier versions. Enhancements and corrections made to subsequent versions of system software will not be available to entities that forgo acquiring the latest version. All system software should have current and complete documentation. Inadequate documentation will hinder maintenance activities, particularly during emergency situations when in-house systems programmers are attempting to restart a failed system and vendor assistance is not readily available.

Control Techniques and Suggested Audit Procedures Critical Element SS-3

Control Activities	Control Techniques	Audit Procedures
SS-3.1 System software changes are authorized, tested, and approved before implementation.	Policies and procedures exist and are up-to-date for identifying, selecting, installing, and modifying system software. Procedures include an analysis of costs and benefits and consideration of the impact on processing reliability and security.	Review pertinent policies and procedures. Interview management and systems personnel.
	Procedures exist for identifying and documenting system software problems. This should include using a log to record the problem, the name of the individual assigned to analyze the problem, and how the problem was resolved.	Review procedures for identifying and documenting system software problems. Interview management and systems programmers. Review the causes and frequency of any recurring system software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems.
	New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document.	Determine what authorizations and documentation are required prior to initiating system software changes. Select recent system software changes and determine whether the authorization was obtained and the change is supported by a change request document.
	New system software versions or products and modifications to existing system software are tested and the test results are approved before implementation. Procedures include: • a written standard that guides the testing, which is conducted in a test rather than production environment; • specification of the optional security-related features to be turned on, when appropriate; • review of test results by technically qualified staff who document their opinion on whether the system software is ready for production use; and • review of test results and documented opinions by data center management prior to granting approval to move the system software into production use.	Determine the procedures used to test and approve system software prior to its implementation. Select recent system software changes and test whether the indicated procedures were in fact used.
	Procedures exist for controlling emergency changes. Procedures include: • authorizing and documenting emergency changes as they occur; • reporting the changes for management review; and • review by an independent IS supervisor of the change.	Review procedures used to control and approve emergency changes. Select emergency changes to system software and test whether the indicated procedures were in fact used.

Control Techniques and Suggested Audit Procedures Critical Element SS-3

Control Activities	Control Techniques	Audit Procedures
SS-3.2 Installation of system software is documented and reviewed.	Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.	Interview management and systems programmers about scheduling and giving advance notices when system software is installed. Review recent installations and determine whether scheduling and advance notification did occur. Determine whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.
	Migration of tested and approved system software to production use is performed by an independent library control group. Outdated versions of system software are removed from production libraries.	Interview management, systems programmers, and library control personnel, and determine who migrates approved system software to production libraries and whether outdated versions are removed from production libraries. Review supporting documentation for some system software migrations and the removal of outdated versions from production libraries.
	Installation of all system software is logged to establish an audit trail and reviewed by data center management.	Interview data center management about their role in reviewing system software installations. Review some recent system software installations and determine whether documentation shows that logging and management review occurred.
	Vendor-supplied system software is still supported by the vendor.	Interview system software personnel concerning a selection of system software and determine the extent to which the operating version of the system software is currently supported by the vendor.
	All system software is current and has current and complete documentation.	Interview management and systems programmers about the currency of system software and the currency and completeness of software documentation. Review documentation and test whether recent changes are incorporated.

Sources of Additional Information on System Software

Information Systems Audit and Control Foundation, CobiT: Control Objectives for Information and Related Technology, 1998.

Lainhart and Donahue, The Information Systems Control Foundation, Computerized Information Systems (CIS) Audit Manual: A Guide to CIS Auditing in Government Organizations, July 1992 (pp. IC-3.26-IC-3.28).

The Information Systems Control Foundation, Control Objectives: Controls in an Information Systems Environment - Objectives, Guidelines, and Audit Procedures, April 1992 (pp. I-3-11-I-3-13).

The Institute of Internal Auditors Research Foundation, Systems Auditability and Control: Module 4 - Managing Computer Resources, April 1991 (pp. 95-109).

3.5 SEGREGATION OF DUTIES (SD)

Work responsibilities should be segregated so that one individual does not control all critical stages of a process. For example, while users may authorize program changes, programmers should not be allowed to do so because they are not the owners of the system and do not have the responsibility to see that the system meets user needs. Similarly, one computer programmer should not be allowed to independently write, test, and approve program changes. Often, segregation of duties is achieved by splitting responsibilities between two or more organizational groups. Dividing duties among two or more individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other.

Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed. For example,

- an individual who was independently responsible for authorizing, processing, and reviewing payroll transactions could inappropriately increase payments to selected individuals without detection or
- a computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.

The extent to which duties are segregated depends on the size of the organization and the risk associated with its facilities and activities. A large organizations will have more flexibility in separating key duties than a small organization that must depend on only a few individuals to perform its operations. These smaller organization may rely more extensively on supervisory review to control activities. Similarly, activities that involve extremely large dollar transactions, or are otherwise inherently risky, should be divided among several individuals and be subject to relatively extensive supervisory review.

Key areas of concern during a general controls review involve the segregation of duties among major operating and programming activities, including duties performed by users, application programmers, and data center staff. Policies outlining the responsibilities of these groups and related individuals should be documented, communicated, and enforced.

Because of the nature of computer operations, segregation of duties alone will not ensure that personnel only perform authorized activities, especially computer

operators. To help prevent or detect unauthorized or erroneous personnel actions requires effective supervision and review by management and formal operating procedures.

Determining whether duties are adequately segregated and the activities of personnel are adequately controlled involves assessing the entity's efforts to perform each of the critical elements listed below.

Critical Elements	
SD-1	Segregate incompatible duties and establish related policies
SD-2	Establish access controls to enforce segregation of duties
SD-3	Control personnel activities through formal operating procedures and supervision and review

Critical Element SD-1: Segregate incompatible duties and establish related policies

The first steps in determining if duties are appropriately segregated are to analyze the entity's operations, identify incompatible duties, and assign these duties to different organizational units or individuals. Federal internal control standards specify that key duties and responsibilities for authorizing, processing, recording, and reviewing transactions should be separated. This concept can also be applied to the authorization, testing, and review of computer program changes.

Segregating duties begins by establishing independent organizational groups with defined functions, such as a payroll unit responsible for preparing payroll transaction input and a data processing unit responsible for processing input prepared by other units. Functions and related tasks performed by each unit should be documented for the unit and in staff job descriptions and should be clearly communicated to personnel assigned the responsibilities.

SD-1.1: Incompatible duties have been identified and policies implemented to segregate these duties

Management should have analyzed operations and identified incompatible duties that are then segregated through policies and organizational divisions. Although incompatible duties may vary from one entity to another, the following functions are generally performed by different individuals: IS management, systems design, application programming, systems programming, quality assurance/testing, library management/change management, computer operations, production control and scheduling, data security, data administration, and network administration. A brief description of these functions follows.

IS management includes the personnel who direct or manage the activities and staff of the IS department and its various organizational components.

Systems design is the function of identifying and understanding user information needs and translating them into a requirements document that is used to build a system.

Application programming involves the development and maintenance of programs for specific applications, such as payroll, inventory control, accounting, and mission support systems.

Systems programming involves the development and maintenance of programs that form the systems software, such as operating systems, utilities, compilers, and security software.

Quality assurance/testing is the function that reviews and tests newly developed systems and modifications to determine whether they function as specified by the user and perform in accordance with functional specifications. Testing may also determine whether appropriate procedures, controls, and documentation have been developed and implemented before approval is granted to place the system into operation.

Library management/change management is the function responsible for control over program and data files that are either kept on-line or are on tapes and disks that are loaded onto the computer as needed. Software programs are generally used to assist in the control of these files. This function also is often responsible for controlling documentation related to system software, application programs, and computer operations.

Computer operations is the function responsible for performing the various tasks to operate the computer and peripheral equipment, including providing the tape, disk, or paper resources as requested by the application systems.

Production control and scheduling is the function responsible for monitoring the information into, through, and as it leaves the computer operations area and for determining the succession of programs to be run on the computer. Often, an automated scheduling package is utilized in this task. An entity may have a separate **Data control** group that is responsible for seeing that all data necessary for processing is present and that all output is complete and distributed properly. This group is generally also responsible for reconciling record counts and control totals submitted by users with similar counts and totals generated during processing.

Data security is the function responsible for the development and administration of an entity's information security program. This includes development of security policies, procedures, and guidelines and the establishment and maintenance of a security awareness and education program for employees. The data security function is also concerned with the adequacy of access controls and service continuity procedures.

Data administration is the function that plans for and administers the data used throughout the entity. This function is concerned with identifying, cataloging, controlling, and coordinating the information needs of the entity. Database administration is a narrower function concerned with the technical aspects of

installing, maintaining, and using an entity's databases and database management systems.

Network Administration is the function responsible for maintaining a secure and reliable on-line communications network and serves as liaison with user departments to resolve network needs and problems.

The following include examples of restrictions that are generally addressed in policies about segregating duties and are achieved through organizational divisions and access controls.

- Application users should not have access to operating system or application software.
- Programmers should not be responsible for moving programs into production or have access to production libraries or data.
- Access to operating system documentation should be restricted to authorized systems programming personnel.
- Access to application system documentation should be restricted to authorized applications programming personnel.
- Access to production software libraries should be restricted to library management personnel.
- Persons other than computer operators should not set up or operate the production computer.
- Only users, not computer staff, should be responsible for transaction origination or correction and for initiating changes to application files.
- Computer operators should not have access to program libraries or data files.

Some steps involved in processing a transaction also need to be separated among different individuals. For example, the following combinations of functions should not be performed by a single individual.

- Data entry and verification of data,
- Data entry and its reconciliation to output,
- Input of transactions for incompatible processing functions (e.g., input of vendor invoices and purchasing and receiving information), and
- Data entry and supervisory authorization functions (e.g., authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's review and approval.)

Organizations with limited resources to segregate duties should have compensating controls, such as supervisory review of transactions performed.

SD-1.2: Job descriptions have been documented

Documented job descriptions should exist that clearly describe employee duties and prohibited activities. These should include responsibilities that may be assumed during emergency situations. The documented job descriptions should match employees' assigned duties. Also, they should include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and should be useful for hiring, promoting, and performance evaluation purposes.

SD-1.3: Employees understand their duties and responsibilities

Employees and their supervisors should understand their responsibilities and the activities that are prohibited. Ultimate responsibility for this rests with senior managers. They should provide the resources and training so that employees understand their responsibilities and ensure that segregation of duty principles are established, enforced, and institutionalized within the organization.

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

Control Activities	Control Techniques	Audit Procedures
SD-1.1 Incompatible duties have been identified and policies implemented to segregate these duties.	Policies and procedures for segregating duties exist and are up-to-date.	Review pertinent policies and procedures. Interview selected management and IS personnel regarding segregation of duties.
	Distinct systems support functions are performed by different individuals, including the following: • IS management. • System design. • Application programming. • Systems programming. • Quality assurance/testing. • Library management/change management. • Computer operations. • Production control and scheduling. • Data control. • Data security. • Data administration. • Network administration.	Review an agency organization chart showing IS functions and assigned personnel. Interview selected personnel and determine whether functions are appropriately segregated. Determine whether the chart is current and each function is staffed by different individuals. Review relevant alternate or backup assignments and determine whether the proper segregation of duties is maintained. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.
	No individual has complete control over incompatible transaction processing functions. Specifically, the following combination of functions are not performed by a single individual: • Data entry and verification of data. • Data entry and its reconciliation to output. • Input of transactions for incompatible processing functions (e.g., input of vendor invoices and purchasing and receiving information). • Data entry and supervisory authorization functions (e.g., authorizing a rejected transaction to continue processing that exceeds some limit. requiring a supervisor's review and approval).	Review the organizational chart and interview personnel to determine that assignments do not result in a single person being responsible for the indicated combinations of functions. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.
	Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.	Interview management, observe activities, and test transactions. *Note: Perform this in conjunction with SD-3.2.*
	Data processing personnel are not users of information systems. They and security mangers do not initiate, input, or correct transactions.	Determine through interview and observation whether data processing personnel and security managers are prohibited from these activities.
	Day-to-day operating procedures for the data center are adequately documented and prohibited actions are identified.	Review the adequacy of documented operating procedures for the data center.

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

Control Activities	Control Techniques	Audit Procedures
SD-1.1 Incompatible duties have been identified and policies implemented to segregate these duties. (Continued)	Regularly scheduled vacations and periodic job/shift rotations are required (see SP-4.1 on personnel policies).	*Audit procedures are found in section SP-4.1, but this item is listed here as a reminder. Individuals performing incompatible duties and acting inappropriately could be detected when another individual undertakes those duties. Requiring vacations and rotations helps detect such actions.*
SD-1.2 Job descriptions have been documented.	Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.	Review job descriptions for several positions in organizational units and for user security administrators. Determine whether duties are clearly described and prohibited activities are addressed. Review the effective dates of the position descriptions and determine whether they are current. Compare these descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.
	Documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and can be used for hiring, promoting, and performance evaluation purposes.	Review job descriptions and interview management personnel.
SD-1.3 Employees understand their duties and responsibilities.	All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.	Interview personnel filling positions for the selected job descriptions (see above). Determine if the descriptions match their understanding of their duties and responsibilities and whether additional duties are undertaken that are not listed in their job descriptions.
	Senior management is responsible for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization.	Determine from interviewed personnel whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.
	Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood, and followed.	Interview management personnel in these activities.

Critical Element SD-2: Establish access controls to enforce segregation of duties

Once policies and job descriptions have been developed that support segregation of duties, controls should be implemented to ensure that these policies are followed.

SD-2.1: Physical and logical access controls have been established

Both physical and logical access controls can be used to enforce many entity policies regarding segregation of duties and should be based on organizational and individual job responsibilities. (Access control is discussed in detail in section 3.2.) For example, logical access controls can preclude computer programmers from using applications software or accessing computerized data associated with applications. Similarly, physical access controls, such as key cards and a security guard, can be used to prevent unauthorized individuals from entering a data processing center.

SD-2.2: Management reviews effectiveness of control techniques

Periodic management reviews are essential to make certain employees are performing their duties in accordance with established policies. Such reviews also help identify the need to update policies when operational processes change.

In particular, management should periodically review activities that cannot be controlled by physical or logical access controls. Such activities are typically controlled instead by supervisory oversight and documentation showing approvals and authorizations. (See critical element SD-3 for more detail on supervision.)

Control Techniques and Suggested Audit Procedures for Critical Element SD-2		
Control Activities	**Control Techniques**	**Audit Procedures**
SD-2.1 Physical and logical access controls have been established.	Physical and logical access controls help restrict employees to authorized actions based upon organizational and individual job responsibilities.	Interview management and subordinate personnel. *Note: This audit step should be performed in conjunction with audit steps in section AC-3.*
SD-2.2 Management reviews effectiveness of control techniques.	Staff's performance should be monitored on a periodic basis and controlled to ensure that objectives laid out in job descriptions are carried out.	Interview management and subordinate personnel. Select documents or actions requiring supervisory review and approval for evidence of such performance (e.g., approval of input of transactions, software changes).
	Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).	Determine which reviews are conducted to assess the adequacy of duty segregation. Obtain and review results of such reviews. *Note: This audit step should be performed in conjunction with audit steps in critical elements SP-1 and SP-5.*

Critical Element SD-3: Control personnel activities through formal operating procedures and supervision and review

Control over personnel activities requires formal operating procedures and active supervision and review of these activities. This is especially relevant for computer operators. Inadequacies in this area could allow mistakes to occur and go undetected and facilitate unauthorized use of the computer.

SD-3.1: Formal procedures guide personnel in performing their duties

Detailed, written instructions should exist and be followed to guide personnel in performing their duties. These instructions are especially important for computer operators. For example, computer operator instruction manuals should provide guidance on system startup and shut down procedures, emergency procedures, system and job status reporting, and operator prohibited activities. Application-specific manuals (commonly called run manuals) should provide additional instructions for operators specific to each application, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures. Operators should be prevented from overriding file label or equipment error messages.

SD-3.2: Active supervision and review are provided for all personnel

Supervision and review of personnel activities help make certain that these activities are performed in accordance with prescribed procedures, that mistakes are corrected, and that the computer is used only for authorized purposes. To aid in this oversight, all computer operator activities on the computer system should be recorded on an automated history log, which serves as an audit trail. Supervisors should routinely review this history log and investigate any abnormalities.

The actions taken by operators during system startup should be particularly monitored as parameters set during the initial program load (IPL) establishes the environment in which the computer operates and security features at startup could be disabled or not activated.

Control Techniques and Suggested Audit Procedures for Critical Element SD-3		
Control Activities	**Control Techniques**	**Audit Procedures**
SD-3.1 Formal procedures guide personnel in performing their duties.	Detailed, written instructions exist and are followed for the performance of work.	Review manuals. Interview supervisors and personnel. Observe processing activities.
	Operator instruction manuals provide guidance on system operation.	
	Application run manuals provide instruction on operating specific applications.	
	Operators are prevented from overriding file label or equipment error messages.	
SD-3.2 Active supervision and review are provided for all personnel.	Personnel are provided adequate supervision and review, including each shift for computer operations.	Interview supervisors and personnel Observe processing activities. Review history log reports for signatures indicating supervisory review. Determine who is authorized to perform the initial program load for the system, what steps are followed, and what controls are in place to monitor console activity during the process. Determine whether operators override the IPL parameters.
	All operator activities on the computer system are recorded on an automated history log.	
	Supervisors routinely review the history log and investigate any abnormalities.	
	System startup is monitored and performed by authorized personnel. Parameters set during the initial program load (IPL) are in accordance with established procedures.	

Sources of Additional Information on Segregation of Duties

Information Systems Audit and Control Foundation, CobiT: Control Objectives for Information and Related Technology, 1998.

Standards For Internal Controls In The Federal Government, U. S. General Accounting Office, (GAO/AIMD-98-21.3.1, December 1997).

Lainhart and Donahue, The Information Systems Control Foundation, Computerized Information Systems (CIS) Audit Manual: A Guide to CIS Auditing in Government Organizations, July 1992 (pp. IC-1.14 - IC-1.19, and IC-3.4 - IC-3.6).

The Information Systems Control Foundation, Control Objectives: Controls in an Information Systems Environment - Objectives, Guidelines, and Audit Procedures, April 1992 (p. I-1-6).

The Institute of Internal Auditors Research Foundation, Systems Auditability and Control: Module 4 - Managing Computer Resources, April 1991 (pp. 24 & 27).

[This page intentionally left blank.]

3.6 SERVICE CONTINUITY (SC)

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as the activities performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises.

Although often referred to as disaster recovery plans, controls to ensure service continuity should address the entire range of potential disruptions. These may include relatively minor interruptions, such as temporary power failures, as well as major disasters, such as fires or natural disasters that would require reestablishing operations at a remote location, and may also include errors, such as writing over a file. If controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information. For some operations, such as those involving health care or safety, system interruptions could also result in injuries or loss of life.

To mitigate service interruptions, it is essential that the related controls be understood and supported by management and staff throughout the organization. Senior management commitment is especially important to ensure that adequate resources are devoted to emergency planning, training, and related testing. In addition, all staff with service continuity responsibilities, such as staff responsible for backing up files, should be fully aware of the risks of not fulfilling these duties.

Assessing service continuity controls involves evaluating the entity's performance in each of the critical elements listed below.

Critical Elements

SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources

SC-2 Take steps to prevent and minimize potential damage and interruption

SC-3 Develop and document a comprehensive contingency plan

SC-4 Periodically test the contingency plan and adjust it as appropriate

Critical Element SC-1: Assess the criticality and sensitivity of computerized operations and identify supporting resources

At most entities, the continuity of certain automated operations is more important than others, and it is not cost-effective to provide the same level of continuity for all operations. For this reason, it is important that management analyze data and operations to determine which are the most critical and what resources are needed to recover and support them. This is the first step in determining which resources merit the greatest protection and what contingency plans need to be made.

SC-1.1: Critical data and operations are identified and prioritized

The criticality and sensitivity of various data and operations should be determined and prioritized based on an overall risk assessment of the entity's operations. As discussed in section 3.1, Entitywide Security Program Planning and Management, such a risk assessment should serve as the foundation of an entity's security plan. Factors to be considered include the importance and sensitivity of the data and other organizational assets handled or protected by the individual operations and the cost of not restoring data or operations promptly. For example, a 1-day interruption of major tax or fee collection systems or a loss of related data could significantly slow or halt receipt of revenues, diminish controls over millions of dollars in receipts, and reduce public trust. Conversely, a system that monitors employee training could be out of service for perhaps as much as several months without serious consequences. Also, sensitive data, such as personal information on individuals or information related to contract negotiations, may require special protection during a suspension of normal service even if such information is not needed on a daily basis to carry out critical operations.

Generally, critical data and operations should be identified and ranked by personnel involved in an entity's business or program operations. Managers should predict the negative effects of lost data and interrupted operations and determine how long specific operations can be suspended or postponed. However, it is also important to obtain senior management's agreement with such determinations, as well as concurrence from affected groups.

The prioritized listing of critical information resources and operations should be periodically reviewed to determine whether it reflects current conditions. Such reviews should occur whenever there is a significant change in the entity's mission and operations or in the location or design of the systems that support these operations.

SC-1.2: Resources supporting critical operations are identified

Once critical data and operations have been determined, the minimum resources needed to support them should be identified and their role analyzed. The resources to be considered include computer resources, such as computer hardware, software, and data files; computer supplies, including paper stock and preprinted forms; telecommunications services; and any other resources that are necessary to the operation, such as people, office facilities and supplies, and noncomputerized records. For example, an analysis should be performed to identify the maximum number of disk drives needed at one time and the specific requirements for telecommunications lines and devices.

Because essential resources are likely to be held or managed by a variety of groups within an organization, it is important that program and IS support staff work together to identify the resources for critical operations.

SC-1.3: Emergency processing priorities are established

In conjunction with identifying and ranking critical functions, the entity should develop a plan for restoring critical operations. The plan should clearly identify the order in which various aspects of processing should be restored, who is responsible, and what supporting equipment or other resources will be needed. A carefully developed processing restoration plan can help employees immediately begin the restoration process and make the most efficient use of limited computer resources during an emergency. Both system users and data center staff should be involved in determining emergency processing priorities. (See critical element SC-3 for additional information on contingency planning.)

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

Control Activities	Control Techniques	Audit Procedures
SC-1.1 Critical data and operations are identified and prioritized.	A list of critical operations and data has been documented that • prioritizes data and operations, • is approved by senior program managers, and • reflects current conditions.	Review related policies. Review list and any related documentation. Interview program, data processing, and security administration officials. Determine their input and their assessment of the reasonableness of priorities established.

Control Techniques and Suggested Audit Procedures for Critical Element SC-1		
Control Activities	**Control Techniques**	**Audit Procedures**
SC-1.2 Resources supporting critical operations are identified.	Resources supporting critical operations have been identified and documented. Types of resources identified should include • computer hardware, • computer software, • computer supplies, • system documentation, • telecommunications, • office facilities and supplies, and • human resources.	Review related documentation. Interview program and security administration officials.
SC-1.3 Emergency processing priorities are established.	Emergency processing priorities have been documented and approved by appropriate program and data processing managers.	Review related policies. Review related documentation. Interview program and security administration officials.

Critical Element SC-2: Take steps to prevent and minimize potential damage and interruption

There are a number of steps that an organization should take to prevent or minimize the damage to automated operations that can occur from unexpected events. These can be categorized as follows:

- routinely duplicating or backing up data files, computer programs, and critical documents with off-site storage;
- installing environmental controls, such as fire suppression systems or backup power supplies;
- arranging for remote backup facilities that can be used if the entity's usual facilities are damaged beyond use; and
- ensuring that staff and other users of the system understand their responsibilities in case of emergencies.

Taking such steps, especially implementing thorough backup procedures and installing environmental controls, are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters. In particular, an entity should maintain an ability to restore data files, which may be impossible to recreate if lost. In addition, effective maintenance, problem management, and change management for hardware equipment will help prevent unexpected interruptions.

To assess this critical element, the auditor should determine whether the entity performs the following control activities.

SC-2.1: Data and program backup procedures have been implemented

Routinely copying data files and software and securely storing these files at a remote location are usually the most cost-effective actions that an entity can take to mitigate service interruptions. Although equipment can often be readily replaced, the cost could be significant and reconstructing computerized data files and replacing software can be extremely costly and time consuming. Sometimes, reconstruction of data files may be virtually impossible. In addition to the direct costs of reconstructing files and obtaining software, the related service interruptions could lead to significant financial losses.

A program should be in place for regularly backing up computer files, including master files, transaction files, application programs, systems software, and database software and storing these backup copies securely at an off-site location. Although choosing a backup storage location is a matter of judgment, the backup location should be far enough away from the primary location that it will not be impaired by the same events, such as fires, storms, and electrical power outages. In addition, it should be protected from unauthorized access and from environmental hazards, such as fires and power outages.

The frequency with which files should be backed up depends on the volume and timing of transactions that modify the data files. Generally, backing up files on a daily basis is adequate. However, if a system accounts for thousands of transactions per day, it may be appropriate to back up files several times a day. Conversely, if only a few transactions are recorded every week, then weekly back up may be adequate.

File backup procedures should be designed so that a recent copy is always available. For example, new data file versions should be received at the off-site storage location before the disks or tapes containing prior versions are returned to the data center for reuse.

Generally, data center personnel are responsible for routinely backing up files. However, if critical data are routinely maintained on computers that are not under the control of data center personnel, then responsibility for backing up this information should be clearly defined.

In addition to data files and software programs, copies of any other information and supplies that may be needed to maintain operations should be maintained at a remote location. Examples of such documents are system and application documentation, unique preprinted computer paper, and essential legal files. Although a review of computer-related controls focuses on electronically maintained data, it is important that critical paper documents also be copied and stored remotely so that they are available when needed to support automated operations.

SC-2.2: Adequate environmental controls have been implemented

Environmental controls prevent or mitigate potential damage to facilities and interruptions in service. Examples of environmental controls include

- fire extinguishers and fire suppression systems;

- fire alarms;
- smoke detectors;
- water detectors;
- redundancy in air cooling systems;
- backup power supplies;
- existence of shut-off valves and procedures for any building plumbing lines that may endanger processing facilities;
- processing facilities built with fire resistant materials and designed to reduce the spread of fire; and
- policies prohibiting eating, drinking, and smoking within computer facilities.

Environmental controls can diminish the losses from some interruptions such as fires or prevent incidents by detecting potential problems early, such as water leaks or smoke, so that they can be remedied. Also, uninterruptible or backup power supplies can carry a facility through a short power outage or provide time to back up data and perform orderly shut-down procedures during extended power outages.

SC-2.3: Staff have been trained to respond to emergencies

Staff should be trained in and aware of their responsibilities in preventing, mitigating, and responding to emergency situations. For example, data center staff should receive periodic training in emergency fire, water, and alarm incident procedures as well as their responsibilities in starting up and running an alternate data processing site. Also, if outside users are critical to the entity's operations, they should be informed of the steps they may have to take as a result of an emergency.

Generally, information on emergency procedures and responsibilities can be provided through training sessions and by distributing written policies and procedures. Training sessions should be held at least once a year and whenever changes to emergency plans are made.

Also, if staff could be required to relocate or significantly alter their commuting routine in order to operate an alternate site in an emergency, it is advisable for an entity to incorporate into the contingency plan steps for arranging lodging and meals or any other facilities or services that may be needed to accommodate the essential human resources.

SC-2.4: Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions

Unexpected service interruptions can occur from hardware equipment failures or from changing equipment without adequate advance notification to system users. To prevent such occurrences requires an effective program for maintenance, problem management, and change management for hardware equipment.

Routine periodic hardware maintenance should be scheduled and performed to help reduce the possibility and impact of equipment failures. Vendor-supplied specifications normally prescribe the frequency and type of preventative maintenance to be performed. Such maintenance should be scheduled in a manner to minimize the impact on overall operations and on critical or sensitive applications. Specifically, peak workload periods should be avoided. All maintenance performed should be documented, especially any unscheduled maintenance that could be analyzed to identify problem areas warranting additional actions for a more permanent solution. Flexibility should be designed into the data processing operations to accommodate the required preventative maintenance and reasonably expected unscheduled maintenance. For critical or sensitive applications that require a high level of system availability, the acquisition and use of spare or backup hardware may be appropriate.

Effective problem management requires tracking service performance and documenting problems encountered. Goals should be established by senior management on the availability of data processing and on-line service. Records should be maintained on the actual performance in meeting service schedules. Problems and delays encountered, the reasons for the problems or delays, and the elapsed time for resolution should be recorded and analyzed to identify any recurring pattern or trend. Senior management should periodically review and compare the service performance achieved with the goals and survey user departments to see if their needs are being met.

Changes of hardware equipment and related software should be scheduled to minimize the impact on operations and users and allow for adequate testing to demonstrate that they will work as needed. Advance notification should be given to users so that service is not unexpectedly interrupted.

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

Control Activities	Control Techniques	Audit Procedures
SC-2.1 Data and program backup procedures have been implemented.	Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.	Review written policies and procedures for backing up files. Compare inventory records with the files maintained off-site and determine the age of these files. For a selection of critical files, locate and examine the backup files. Verify that backup files can be used to recreate current reports. Determine whether backup files are created and rotated off-site as prescribed and are sent before prior versions are returned.
	System and application documentation are maintained at the off-site storage location.	Locate and examine documentation.
	The backup storage site is • geographically removed from the primary site(s), and • protected by environmental controls and physical access controls.	Examine the backup storage site.
SC-2.2 Adequate environmental controls have been implemented.		*These procedure should be performed in conjunction with Section AC-3.3, regarding physical access controls.*
	Fire suppression and prevention devices have been installed and are working, e.g., smoke detectors, fire extinguishers, and sprinkler systems. Controls have been implemented to mitigate other disasters, such as floods, earthquakes, etc. Redundancy exists in the air cooling system. Building plumbing lines do not endanger the computer facility or, at a minimum, shut-off valves and procedures exist and are known. An uninterruptible power supply or backup generator has been provided so that power will be adequate for orderly shut down.	Examine the entity's facilities. Interview site managers. Observe that operations staff are aware of the locations of fire alarms, fire extinguishers, regular and auxiliary electrical power switches, water shut-off valves, breathing apparatus, and other devices that they may be expected to use in an emergency. Observe the operation, location, maintenance and access to the air cooling systems. Observe whether water can enter through the computer room ceiling or pipes are running through the facility and that there are water detectors on the floor. Determine whether the activation of heat and smoke detectors will notify the fire department.

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

Control Activities	Control Techniques	Audit Procedures
SC-2.2 Adequate environmental controls have been implemented. (continued)	Environmental controls are periodically tested.	Review test policies. Review documentation supporting recent tests of environmental controls.
	Eating, drinking, and other behavior that may damage computer equipment is prohibited.	Review policies and procedures regarding employee behavior. Observe employee behavior.
SC-2.3 Staff have been trained to respond to emergencies.	All data center employees have received training and understand their emergency roles and responsibilities. Data center staff receive periodic training in emergency fire, water, and alarm incident procedures. Emergency response procedures are documented.	Interview data center staff. Review training records. Review training course documentation. Review emergency response procedures.
	Emergency procedures are periodically tested.	Review test policies. Review test documentation. Interview data center staff.
SC-2.4 Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	Policies and procedures exist and are up-to-date.	Review policies and procedures.
	Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations.	Interview data processing and user management. Review maintenance documentation.
	Regular and unscheduled maintenance performed is documented.	
	Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled maintenance.	
	Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.	Interview data center management.
	Goals are established by senior management on the availability of data processing and on-line services.	Interview senior management, data processing management, and user management. Review supporting documentation.
	Records are maintained on the actual performance in meeting service schedules.	
	Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.	

Control Techniques and Suggested Audit Procedures for Critical Element SC-2		
Control Activities	**Control Techniques**	**Audit Procedures**
SC-2.4 Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions. (continued)	Senior management periodically reviews and compares the service performance achieved with the goals and surveys user departments to see if their needs are being met.	Interview senior management, data processing management, and user management. Review supporting documentation.
	Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users thus allowing for adequate testing.	
	Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.	

CRITICAL ELEMENT SC-3: Develop and document a comprehensive contingency plan

A contingency plan should be developed for restoring critical applications that includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. It is important that these plans be clearly documented, communicated to affected staff, and updated to reflect current operations. Testing the plan is addressed in critical element SC-4.

SC-3.1: An up-to-date contingency plan has been documented

Contingency plans should be documented, agreed on by both user and data processing departments, and communicated to affected staff.

The plan should reflect the risks and operational priorities that the entity has identified. In this regard, it should be designed so that the costs of contingency planning do not exceed the costs associated with risks that the plan is intended to reduce.

The plan should be detailed enough so that its success does not depend on the knowledge or expertise of one or two individuals. In this regard, it should identify and provide information on

- supporting resources that will be needed,
- roles and responsibilities of those who will be involved in recovery activities,
- arrangements for off-site disaster recovery location and travel and lodging for necessary personnel, if needed,
- off-site storage location for backup files, and
- procedures for restoring critical applications and their order in the restoration process. (See section SC-1.3 for additional information on emergency processing priorities.)

Multiple copies of the contingency plan should be available with some stored at off-site locations to make sure they are not destroyed by the same events that made the primary data processing facilities unavailable.

SC-3.2: Arrangements have been made for alternate data processing and telecommunications facilities

Depending on the degree of service continuity needed, choices for alternative facilities will range from an equipped site ready for immediate backup service, referred to as a "hot site," to an unequipped site that will take some time to prepare for operations, referred to as a "cold site." In addition, various types of services can be prearranged with vendors. These include making arrangements with suppliers of computer hardware and telecommunications services as well as with suppliers of business forms and other office supplies.

As with all emergency preparations, costs and risks should be considered in deciding what type of alternate site is needed. However, it should be geographically removed from the original site so that it is not subject to impairment from the same events. For example, if the original site and the alternate site are separated geographically, it is unlikely that they would both be damaged by the same flood, fire, or earthquake. In addition, the site should have ready access to the basic utilities needed to resume operations, such as electricity, water, and telecommunications services. In some cases, two or more entities will share the same alternate site in order to reduce the cost. However, this may cause problems if two or more entities need the site at the same time.

Whatever options are determined to be the most appropriate, the entity should have a formal agreement or contract detailing the emergency arrangements. Further, the arrangements should be periodically reviewed to determine whether they remain adequate to meet the entity's needs.

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

Control Activities	Control Techniques	Audit Procedures
SC-3.1 An up-to-date contingency plan is documented.	A contingency plan has been documented that • reflects current conditions, • has been approved by key affected groups including senior management, data center management, and program managers, • clearly assigns responsibilities for recovery, • includes detailed instructions for restoring operations (both operating system and critical applications), • identifies the alternate processing facility and the backup storage facility, • includes procedures to follow when the data/service center is unable to receive or transmit data, • identifies critical data files, • is detailed enough to be understood by all agency managers, • includes computer and telecommunications hardware compatible with the agencies needs, and • has been distributed to all appropriate personnel.	Review the contingency plan and compare its provisions with the most recent risk assessment and with a current description of automated operations. Interview senior management, data center management, and program managers.
	The plan provides for backup personnel so that it can be implemented independent of specific individuals. User departments have developed adequate manual/peripheral processing procedures for use until operations are restored.	Review the contingency plan. Interview senior management, data center management, and program managers.
	Several copies of the current contingency plan are securely stored off-site at different locations.	Observe copies of the contingency plan held off-site.
	The contingency plan is periodically reassessed and, if appropriate, revised to reflect changes in hardware, software, and personnel.	Review the plan and any documentation supporting recent plan reassessments.
SC-3.2 Arrangements have been made for alternate data processing and telecommunications facilities.	Contracts or interagency agreements have been established for a backup data center and other needed facilities that • are in a state of readiness commensurate with the risks of interrupted operations, • have sufficient processing capacity, and • are likely to be available for use. Alternate telecommunication services have been arranged. Arrangements are planned for travel and lodging of necessary personnel, if needed.	Review contracts and agreements.

Critical Element SC-4: Periodically test the contingency plan and adjust it as appropriate

Testing contingency plans is essential to determine whether they will function as intended in an emergency situation. According to OMB, federal managers have reported that testing revealed important weaknesses in their plans, such as backup facilities that could not adequately replicate critical operations as anticipated. Through the testing process, these plans were substantially improved.[1]

The most useful tests involve simulating a disaster situation to test overall service continuity. Such a test would include testing whether the alternative data processing site will function as intended and whether critical computer data and programs recovered from off-site storage are accessible and current. In executing the plan, managers will be able to identify weaknesses and make changes accordingly. Moreover, tests will assess how well employees have been trained to carry out their roles and responsibilities in a disaster situation.

SC-4.1: The plan is periodically tested

The frequency of contingency plan testing will vary depending on the criticality of the entity's operations. Generally, contingency plans for very critical functions should be fully tested about once every year or two, whenever significant changes to the plan have been made, or when significant turnover of key people has occurred. It is important for top management to assess the risk of contingency plan problems and develop and document a policy on the frequency and extent of such testing.

SC-4.2: Test results are analyzed, and the plan is adjusted accordingly

Contingency test results provide an important measure of the feasibility of the contingency plan. As such, they should be reported to top management so that the need for modification and additional testing can be determined and so that top management is aware of the risks of continuing operations with an inadequate contingency plan.

---

[1]"Observations of Agency Computer Security Practices and Implementation of OMB Bulletin No. 90-08: 'Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information'," February 1993.

Any test of contingency plans is likely to identify weaknesses in the plan, and it is important that the plan and related supporting activities, such as training, be revised to address these weaknesses. Otherwise, the benefits of the test will be largely lost.

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

Control Activities	Control Techniques	Audit Procedures
SC-4.1 The plan is periodically tested.	The current plan has been tested under conditions that simulate a disaster.	Review policies on testing. Review test results. Observe a disaster recovery test.
SC-4.2 Test results are analyzed and contingency plans are adjusted accordingly.	Test results were documented and a report, such as a "lessons learned" report, was developed and provided to senior management.	Review final test report. Interview senior managers to determine if they are aware of the test results.
	The contingency plan and related agreements and preparations were adjusted to correct any deficiencies identified during testing.	Review any documentation supporting contingency plan adjustments.

Sources of Additional Information On Service Continuity Controls

Information Systems Audit and Control Foundation, CobiT: Control Objectives for Information and Related Technology, 1998.

NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, December 1995.

Lainhart and Donahue, The Information Systems Control Foundation, Computerized Information Systems (CIS) Audit Manual: A Guide to CIS Auditing in Government Operations, July 1992.

The Institute of Internal Auditors Research Foundation, Systems Auditability and Control: Module 10 - Contingency Planning, April 1991.

CHAPTER 4

EVALUATING AND TESTING APPLICATION CONTROLS

[This chapter is under development and will be issued with the first update to this manual.]

[This page intentionally left blank.]

BACKGROUND INFORMATION QUESTIONNAIRE
General Section

The auditor should gain a basic understanding of how the entity or program under review is supported by automated systems. This background information appendix should serve as a checklist to gain this understanding. To facilitate gathering the information, the following two sections (Background Information - Organization; and Background Information - Operations) are designed to be given to and filled out by IRM management personnel at the entity.

In addition to organization and operations information provided by the entity, the auditor should gather the following information.

Internal and external audits, reviews, and studies

Audits, reviews, and studies are important management tools. The extent to which the entity takes advantage of these management tools and uses them to take corrective actions should be analyzed to identify potential weaknesses that could affect the entity's information management and technology activities. Copies of documents that address information or IRM problems completed during the last 3-5 years, or summaries of ongoing or planned work should be obtained, including the documents listed below.

Document	Workpaper Reference
GAO reports	
Office of Inspector General or internal audit reports	
Internal reviews and studies (e.g., FMFIA, risk analyses)	
Contractor or consultant studies	
Reports of congressional hearings or copies of congressional testimony	
Summaries of ongoing or planned audits, reviews, or studies	

Significance and nature of programs and functions supported by automated systems

The auditor may use a variety of sources to gain a basic understanding of the programs and functions supported by automated systems. These include the sources listed below.

Source	Workpaper Reference
Strategic and tactical IRM plans	
A list of the entity's major automated information systems as defined and required by OMB Circular A-130	
The entity's mission statement	
Bills, acts, titles, or laws that affect the entity and its automated applications	
Pamphlets, brochures, newsletters, booklets, etc., that describe the entity's operations and automated applications	

BACKGROUND INFORMATION QUESTIONNAIRE
Organization Section

Entity _____ Job Code _____

To expedite GAO's review of IRM controls, please complete, sign, and return this form. All blanks should be completed or reviewed by the entity's IRM official. If blanks are not applicable to your environment, please indicate with "N/A."

A. Overview Diagram

Please provide an overview diagram that describes the overall physical IRM environment used for producing or supporting the entity's financial reports. This should include a pictorial representation of (1) major inputs and entry points, (2) major outputs and output points, (3) data flows, (4) processing sites, and (5) communication networks.

For multiple sites (e.g., centralized software development, multiple data center processing), please complete the remainder of this form separately for each site.

B. Organization and Staffing

1. Please attach a copy of the current IRM organization chart.

2. Please provide the name and position of the person to whom the IRM manager reports.

   Name _____ Position _____

3. Please provide the following IRM staffing information.

	Positions		Key contact	
	Authorized	Filled	Name	Phone number
General management				
Security				
Technical support				
System/executive software				
Telecommunications/network maintenance control				
Data administration				
Database administration				
Quality assurance				
Other				
Application maintenance & development				
Systems Planning / Resource Management				
Computer Operations				
Operations				
Librarians				
Production Control				
PC Administration				
LAN/WAN Administration				
Data Entry				
Other				
Total IRM Personnel				

4. Please describe any significant turnover in key IRM positions, and/or organizational consolidations or reorganizations during the past year or anticipated during the coming year.

_____

_____

_____

_____

_____

_____

5. Please attach a copy of the current year IRM organization budget, together with the most current year-to-date actual versus budget comparison.

C. Computer Operations

1. Number of scheduled 8-hour shifts per day _____

2. Number of scheduled days per week _____

3. Average number of jobs processed per day _____

4. Does the data center operate without staff on-site ("dark or dim", "lights-out", "unattended operations")? [] Yes [] No

   If yes, for which shifts?

   _____

   _____

5. Please describe any IRM function, other than computer operations, that has more than one standard shift:

Name of group _____

Number of shifts _____

D. Continuity of Service

1. Does the installation have a contingency plan? [] Yes [] No

   If yes, please attach a summary of the plan, if available.

2. Does the installation have an off-site storage facility? [] Yes [] No

   If yes, please attach a summary of the off-site storage policy, if available.

3. Does the installation have an uninterruptible power source? [] Yes [] No

   If so, what is the duration and kind of power source?

   _____

   _____

4. What is the date and results of the last test of the contingency plan?

   _____

   _____

5. What is the date of the last audit of the off-site storage facility?

   _____

   _____

Appendix I

E. Signature Blocks

Please complete the following signature blocks.

Prepared by _____

Position/title _____

Date _____

Telephone number _____

Fax number _____

Reviewed by _____

Position/title _____

Date _____

Telephone number _____

Fax number _____

BACKGROUND INFORMATION QUESTIONNAIRE
Operations Section

Entity _____ Job Code _____

Please complete one form for each central processing unit (CPU) that is used to process financial data used to produce or support the entity's financial reports.

A. Processing Environment Diagram

Please provide a diagram to help GAO understand the physical IRM environment used to process financial data used to produce or support the entity's financial reports. This should include a pictorial representation of (1) the CPU and major peripherals, (2) the telecommunications system–modems, terminals (dumb, intelligent), communication links (type, speed), and (3) network(s) (LAN/WAN) including topology (ring, bus/tree).

B. CPU

Manufacturer/model _____

Year acquired _____

Operating system _____

Release number _____

Memory storage capacity _____

If the CPU is logically divided into multiple processing areas (e.g., regions, domains), please list and describe each area

_____

_____

_____

_____

Please provide the physical building location.

_____

_____

C. Peripherals

	Number	Capacity
Master console(s)		
Direct access storage devices		
Other storage devices (specify type _____)		
Optical scanners		
Modem units (specify baud rate _____)		
MICR readers		
Key-to-tape units		
Key-to-disk units		
High-speed printers		
Communications controllers (specify type_____)		
Other		

D. Intelligent Terminals (e.g., IBM PC)

Number	Location	Purpose

E. Dumb Terminals (e.g., IBM 3278)

Number	Location	Purpose

F. Telecommunications

1. Does the entity use cooperative processing (i.e., do separate portions of an application reside on different computers)? [] Yes [] No

   If yes, describe how cooperative processing is used.

2. Does the entity use dial-up lines? [] Yes [] No

   If yes, describe how dial-up lines are used.

3. Does the entity use leased lines? [] Yes [] No

   If yes, describe how leased lines are used.

4. Is there a Local Area Network (LAN)? [] Yes [] No

   If yes, describe how the LAN is used.

5. Is there a Wide Area Network (WAN)? [] Yes [] No

   If yes, describe how the WAN is used.

   _____

   _____

6. Is Electronic Data Interchange (EDI) used? [] Yes [] No

   If yes, describe how EDI is used.

   _____

   _____

7. Are Electronic Fund Transfers initiated or processed by the computer? [] Yes [] No

8. Does the entity use data encryption for all transmission of data? [] Yes [] No

G. Systems Software

Some of the more commonly used system software is listed below. Please (1) check the software used in your environment, (2) respond in the space provided, if not listed, or (3) indicate "N/A", if not applicable.

1. Online monitor

	Number of production regions	Is security interfaced with access control software (#7 below)?
[] IMS/DC	_____	[] Yes [] No
[] CICS	_____	[] Yes [] No
[] _____	_____	[] Yes [] No

2. Tape management system
   - [] CA-1
   - [] TMS
   - [] EPAT
   - [] _____

3. Program library software (source code)
   - [] PANVALET
   - [] LIBRARIAN
   - [] ENDEAVOR

[] _____

4. Program library software (object code)
   [] PANEXEC
   [] _____

5. Job accounting software
   [] CA-JARS
   [] _____

6. Online program development system

   [] TSO
   [] ROSCOE
   [] ICCF
   [] VOLLIE
   [] ISPF
   [] _____

   Is security interfaced with access control software (#7 below)?
   [] Yes [] No
   [] Yes [] No
   [] Yes [] No
   [] Yes [] No
   [] Yes [] No
   [] Yes [] No

7. Access control software
   [] ACF2
   [] RACF
   [] TOPSECRET
   [] _____

   Implementation mode
   [] ABORT [] _____
   [] ACTIVE [] _____
   [] FAIL [] _____
   [] WARN

8. Database management system
   [] DB2
   [] IMS
   [] IDMS
   [] ADABAS
   [] ORACLE
   [] DATACOM
   [] _____

9. Audit software package
   [] PANAUDIT
   [] EDP AUDITOR
   [] CA-EXAMINE
   [] DYL-280
   [] IDEA
   [] ICUMVS
   [] _____

Appendix I

10. Report writer software
    [] EASYTRIEVE
    [] _____

11. Network master control system
    [] NETMASTER
    [] CA-VMAN
    [] _____

12. Job entry subsystem
    [] JES2
    [] JES3
    [] _____

13. Job scheduling system

    [] CA-7
    [] MANAGER
    [] SCHEDULER
    [] _____

    Is security interfaced with access control software (#7 above)?
    [] Yes [] No
    [] Yes [] No
    [] Yes [] No
    [] Yes [] No

14. Performance monitor
    [] OMEGAMON
    [] RESOLVE
    [] DELTAMON
    [] _____

15. Dial-up security software
    [] DEFENDER
    [] LEEHMA
    [] AUDITOR
    [] _____

16. Online data entry software

    [] CICS
    [] KEYMASTER
    [] _____

    Is security interfaced with access control software (#7 above)?
    [] Yes [] No
    [] Yes [] No
    [] Yes [] No

H. Processing Statistics

Please provide a breakdown of system usage/availability by CPU using the latest available data.

(month/year) _____

Production processing	%
Test processing	%
Rerun	%
Maintenance	%
Idle	%
Unplanned downtime	%
Other _____	%
Total	100%

I. Abnormal Terminations (ABENDS)

Please provide the number of ABENDS using the latest available data.

(month/year) _____

Systems software	%
Application software	%
Hardware	%
Operator error	%
Other _____	%
Total	100%

J. Present Application Software

Please list all major production financial application systems that are (1) processed on the CPU listed in section B or (2) PC-based. Please indicate PC-based systems with "(PC)".

Financial system	Key[1] programmer contact	Month/ year installed	Commercial vendor (specify)/ in-house developed	Processing (batch/ online)[2]	Online[3] processing region	Online[4] transaction security

[1]Please give the name of the IRM person who knows the key files, primary logic, and internal security routines for this system.

[2]Online in this context means either real-time or online transaction entry via CICS with batch updating. For example, specify one of the following: Online Real, Online Entry/Batch, or Batch when data are initially created via a stand-alone, key-to-tape or key-to-disk device and then processed in batch mode.

[3]If the application is online real-time or online transaction entry, specify the name of the CICS, IMS/DC, or IDMS/DC region in which it is processed, or else put N/A.

[4]If the application is online real-time or online transaction entry, specify the exact facility used for online transaction security (e.g., CICS tables, ACF2 general resource rules, RACF resource profiles, or internal application security).

K. Future Application Software

List any major computerized financial application systems undergoing major revisions, being planned for major revisions, in the process of being installed, or planned for installation over the next 1 to 3 years.

Financial system	Target installation date	Commercial vendor (specify)/in-house developed	Mode of processing	
			Batch/online	CPU/PC

L. Other Comments

Please provide us with any other information that will help us better understand your IRM environment.

Appendix I

M. Signature Blocks

Please complete the following signature blocks.

Prepared by _____

Position/title _____

Date _____

Telephone number _____

Fax number _____

Reviewed by _____

Position/title _____

Date _____

Telephone number _____

Fax number _____

[This page intentionally left blank.]

Appendix II

USER SATISFACTION QUESTIONNAIRE
Information System Section

The purpose of this questionnaire is to obtain user evaluations of computerized information systems that are significant to the financial statements. Because users generally have a good grasp of a system's strengths and weaknesses, their dissatisfaction with a system can often help identify problems that the auditor should consider when assessing the effectiveness of system controls.

Date _____

Information System Identification

1. Name of information system _____

2. Identification number (if applicable) _____

3. Organization considered system owner _____

4. Organization responsible for developing and maintaining system

   _____

5. Purpose of system _____

   _____

   _____

User Identification Information Needs

6. Name _____ Phone _____

7. Title _____

8. Organization _____

9. Address _____

10. Please describe the activity performed/managed and the key (critical) objectives your organization must accomplish to meet its overall mission.

_____

_____

_____

11. To accomplish the above objectives, what information is needed?

_____

_____

_____

12. Please rate how critical the information system is to achieving your organization's mission. (circle one number)

1	2	3	4	5	6	7

Not critical Critical

Please explain _____

_____

_____

13. Please identify, describe, and attach copies, if available, of key outputs/reports produced by the information system used to fulfill your responsibilities.

_____

_____

_____

14. Please identify the areas for which the information system is used to fulfill your responsibilities. (check all that apply)

[] Entering transactions
[] Reporting program financial activity
[] Monitoring
[] Evaluating
[] Planning
[] Budgeting
[] Other (please specify) _____

_____

Evaluation by User

15. Please rate the accuracy, completeness, and timeliness of the key information from the system that you rely upon to fulfill your responsibilities. (circle one number on each line)

1	2	3	4	5	6	7

Not accurate Accurate

1	2	3	4	5	6	7

Not complete Complete

1	2	3	4	5	6	7

Not timely Timely

Please explain _____

_____

_____

_____

16. If the information is not accurate, complete, or timely (circle description which applies), how is achievement of the organization's intended objectives affected?

_____

_____

_____

17. What procedures are performed to determine whether the needed information is authorized, accurate, and complete?

_____

_____

_____

18. Is the information ever rerun by the data processing department? [] Yes [] No
If so,

a. How often do reruns occur? _____

b. Why were the reruns necessary? _____

_____

c. How do you make sure that the rerun information is accurate?

_____

19. Please rate your satisfaction with the information system and the information it provides. (circle one number)

1	2	3	4	5	6	7

Dissatisfied Satisfied

User Involvement with the Information System

20. Was anyone from your organization involved in any of the following functions regarding the information system?

Determining user requirements	[] Yes	[] No
Designing the system	[] Yes	[] No
Testing the system	[] Yes	[] No
Identifying needed modifications	[] Yes	[] No

Please explain _____

_____

_____

_____

21. Please explain the procedures for resolving problems identified with the information or the system that produces it and for making system modifications.

_____

_____

_____

_____

22. Please provide any other comments that you believe may be of value.

_____

_____

_____

_____

Appendix II

USER SATISFACTION QUESTIONNAIRE
Computer Output Section

One information system generally produces a number of computer products or reports. The purpose of this questionnaire is to obtain user evaluations of specific computer products that the auditor believes are relevant to the audit. Because users who rely on computer products to perform their duties often become aware of the accuracy and reliability of information contained in the products, the auditor should consider this knowledge when assessing the effectiveness of system controls.

Date _____

Product Identification

1. Title of product _____
2. Identification number _____
3. Type of product (report, on-line file, etc.) _____
4. Information on product to be evaluated _____
5. Frequency product is produced _____

User Identification

6. Name _____ Phone _____
7. Title _____
8. Organization _____
9. Address _____

10. Extent of knowledge about product _____

_____

_____

User Evaluation of Output Product

11. Please identify the activities for which you use this product. (check all that apply)

[] Initiating transactions
[] Compiling reports on program financial activity
[] Monitoring program activity
[] Authorizing data changes in the system
[] Maintaining data controls
[] Other (please specify) _____

_____

12. Please rate the importance of this product in relation to the work in your organization. (circle one number)

1	2	3	4	5	6	7

Not important Important

Please explain _____

_____

_____

13. Please rate the clarity of the product contents. (circle one number)

1	2	3	4	5	6	7

Difficult to understand Easy to understand

14. Please rate the accuracy, completeness, and timeliness of the key information from the system that you rely upon to fulfill your responsibilities. (circle one number on each line)

1	2	3	4	5	6	7

Not accurate Accurate

1	2	3	4	5	6	7

Not complete Complete

1	2	3	4	5	6	7

Not timely Timely

Please explain _____

_____

_____

_____

15. Please check the following statement that best describes the action you take to achieve product accuracy.

[] Identify errors and request new production run
[] Supplement information with manual records
[] Supplement information with automated records
[] No action, use report with errors as best as possible
[] No action needed as product is accurate

Appendix III

TABLES FOR SUMMARIZING WORK PERFORMED IN EVALUATING AND TESTING GENERAL CONTROLS

These tables are provided for the auditor's use in performing the audit. They are a consolidation of the tables of control techniques and related suggested audit procedures that are included after the discussion of each critical element. To reduce documentation and allow the tables to be tailored to individual audits, the tables are available in electronic form from GAO's World Wide Web server. Our Internet address is: **<http://www.gao.gov>**.

The tables can be used as a guide during initial interviews and to document the auditor's preliminary assessment of controls. As the audit progresses, the auditor can continue to use the electronic version of the tables to document controls evaluated and tested, test procedures performed, conclusions, and supporting work paper references.

3.1 ENTITYWIDE SECURITY PROGRAM PLANNING AND MANAGEMENT (SP)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SP-1 Periodically assess risks.	Independent risk assessments are performed and documented on a regular basis or whenever systems, facilities, or other conditions change. The risk assessment considers data sensitivity and integrity and the range of risks to the entity's systems and data. Final risk determinations and related management approvals are documented and maintained on file. (Such determinations may be incorporated in the security program plan, which is discussed in the next section.)	Review risk assessment policies. Review the most recent high-level risk assessment. Review the objectivity of personnel who performed and reviewed the assessment.		
SP-2 Document an entitywide security program plan.				
SP-2.1 A security plan is documented and approved.	A security program plan has been documented that • covers all major facilities and operations, • has been approved by key affected parties, and • covers the topics prescribed by OMB Circular A-130 (general support systems / major applications): •Rules of the system / Application rules •Training / Specialized training •Personnel controls / Personnel security •Incident response capability / - - •Continuity of support / Contingency planning •Technical security / Technical controls •System interconnection / Information sharing • - - / Public access controls	Review the security plan. Determine whether the plan covers the topics prescribed by OMB Circular A-130.		
SP-2.2 The plan is kept current.	The plan is reviewed periodically and adjusted to reflect current conditions and risks.	Review the security plan and any related documentation indicating that it has been reviewed and updated and is current.		

3.1 ENTITYWIDE SECURITY PROGRAM PLANNING AND MANAGEMENT (SP)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SP-3 Establish a security management structure and clearly assign security responsibilities.				
SP-3.1 A security management structure has been established.	The security program plan establishes a security management structure with adequate independence, authority, and expertise.	Review the security plan and the entity's organization chart. Interview security management staff.		
	An information systems security manager has been appointed at an overall level and at appropriate subordinate levels.	Review pertinent organization charts and job descriptions. Interview the security manager.		
SP-3.2 Information security responsibilities are clearly assigned.	The security plan clearly identifies who owns computer-related resources and who is responsible for managing access to computer resources. Security responsibilities and expected behaviors are clearly defined for (1) information resource owners and users, (2) information resources management and data processing personnel, (3) senior management, and (4) security administrators.	Review the security plan.		
SP-3.3 Owners and users are aware of security policies.	An ongoing security awareness program has been implemented. It includes first-time training for all new employees, contractors, and users, and periodic refresher training thereafter. Security policies are distributed to all affected personnel, including system/application rules and expected behaviors.	Review documentation supporting or evaluating the awareness program. Observe a security briefing. Interview data owners and system users. Determine what training they have received and if they are aware of their security-related responsibilities. Review memos, electronic mail files, or other policy distribution mechanisms. Review personnel files to test whether security awareness statements are current. Call selected users, identify yourself as security or network staff, and attempt to talk them into revealing their password.		

3.1 ENTITYWIDE SECURITY PROGRAM PLANNING AND MANAGEMENT (SP)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SP-3.4 An incident response capability has been implemented.	The entity's incident response capability has characteristics suggested by NIST: • use of virus identification software, • an understanding of the constituency being served, • an educated constituency that trusts the incident handling team, • a means of prompt centralized reporting, • response team members with the necessary knowledge, skills, and abilities, and • links to other relevant groups.	Interview security manager, response team members, and system users. Review documentation supporting incident handling activities. Determine qualifications of response team members. *(Note: See also Section 3.2, Critical Element AC-4 on monitoring access and security violations.)*		
SP-4 Implement effective security-related personnel policies.				
SP-4.1 Hiring, transfer, termination, and performance policies address security.	For prospective employees, references are contacted and background checks performed.	Review hiring policies. For a selection of recent hires, inspect personnel records and determine whether references have been contacted and background checks have been performed.		
	Periodic reinvestigations are performed at least once every 5 years, consistent with the sensitivity of the position per criteria from the Office of Personnel Management.	Review reinvestigation policies. For a selection of sensitive positions, inspect personnel records and determine whether background reinvestigations have been performed.		
	Confidentiality or security agreements are required for employees and contractors assigned to work with confidential information.	Review policies on confidentiality or security agreements. For a selection of such users, determine whether confidentiality or security agreements are on file.		

Appendix III

3.1 ENTITYWIDE SECURITY PROGRAM PLANNING AND MANAGEMENT (SP)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SP-4.1 Hiring, transfer, termination, and performance policies address security. (continued)	Regularly scheduled vacations exceeding several days are required, and the individual's work is temporarily reassigned.	Review vacation policies. Inspect personnel records to identify individuals who have not taken vacation or sick leave in the past year. Determine who performed vacationing employee's work during vacation.		
	Regular job or shift rotations are required.	Review job rotation policies. Review staff assignment records and determine whether job and shift rotations occur.		
	Termination and transfer procedures include • exit interview procedures; • return of property, keys, identification cards, passes, etc.; • notification to security management of terminations and prompt revocation of IDs and passwords; • immediately escorting terminated employees out of the entity's facilities; and • identifying the period during which nondisclosure requirements remain in effect.	Review pertinent policies and procedures. For a selection of terminated or transferred employees, examine documentation showing compliance with policies. Compare a system-generated list of users to a list of active employees obtained from personnel to determine if IDs and passwords for terminated employees exist.		
SP-4.2 Employees have adequate training and expertise.	Skill needs are accurately identified and included in job descriptions, and employees meet these requirements.	Review job descriptions for security management personnel, and for a selection of other personnel. For a selection of employees, compare personnel records on education and experience with job descriptions.		
	A training program has been developed.	Review training program documentation.		
	Employee training and professional development are documented and monitored.	Review training records and related documentation showing whether such records are monitored and whether employees are receiving the appropriate training.		

Appendix III

3.1 ENTITYWIDE SECURITY PROGRAM PLANNING AND MANAGEMENT (SP)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SP-5 Monitor the security program's effectiveness and make changes as needed.				
SP-5.1 Management periodically assesses the appropriateness of security policies and compliance with them.	The entity's IS security program is subjected to periodic reviews.	Review the reports resulting from recent assessments, including the most recent FMFIA report.		
	Major applications undergo independent review or audit at least every 3 years.	Determine when last independent review or audit occurred and review results.		
	Major systems and applications are authorized or accredited by the managers' whose missions they support.	Review written authorizations or accreditation statements.		
	Top management initiates prompt action to correct deficiencies.	Review documentation related to corrective actions.		
SP-5.2 Management ensures that corrective actions are effectively implemented.	Corrective actions are tested after they have been implemented and monitored on a continuing basis.	Review the status of prior-year audit recommendations and determine if implemented corrective actions have been tested. Review recent FMFIA reports.		

Appendix III

3.2 ACCESS CONTROL (AC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
AC-1 Classify information resources according to their criticality and sensitivity.				
AC-1.1 Resource classifications and related criteria have been established.	Classifications and criteria have been established and communicated to resource owners.	Review policies and procedures. Interview resource owners.		
AC-1.2 Owners have classified resources.	Resources are classified based on risk assessments; classifications are documented and approved by an appropriate senior official and are periodically reviewed.	Review resource classification documentation and compare to risk assessments. Discuss any discrepancies with appropriate officials.		
AC-2 Maintain a current list of authorized users and their access authorized.				
AC-2.1 Resource owners have identified authorized users and their access authorized.	Access authorizations are • documented on standard forms and maintained on file, • approved by senior managers, and • securely transferred to security managers.	Review pertinent written policies and procedures. For a selection of users (both application user and IS personnel) review access authorization documentation.		
	Owners periodically review access authorization listings and determine whether they remain appropriate.	Interview owners and review supporting documentation. Determine whether inappropriate access is removed in a timely manner.		
	The number of users who can dial into the system from remote locations is limited and justification for such access is documented and approved by owners. (See section AC-3.2 for additional controls over dial-up access.)	For a selection of users with dial-up access, review authorization and justification.		
	Security managers review access authorizations and discuss any questionable authorizations with resource owners.	Interview security managers and review documentation provided to them.		

Appendix III

3.2 ACCESS CONTROL (AC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
AC-2.1 Resource owners have identified authorized users and their access authorized. (continued)	All changes to security profiles by security managers are automatically logged and periodically reviewed by management independent of the security function. Unusual activity is investigated.	Review a selection of recent profile changes and activity logs.		
	Security is notified immediately when system users are terminated or transferred.	Obtain a list of recently terminated employees from Personnel and, for a selection, determine whether system access was promptly terminated.		
AC-2.2 Emergency and temporary access authorization is controlled.	Emergency and temporary access authorizations are • documented on standard forms and maintained on file, • approved by appropriate managers, • securely communicated to the security function; and • automatically terminated after a predetermined period.	Review pertinent policies and procedures. Compare a selection of both expired and active temporary and emergency authorizations (obtained from the authorizing parties) with a system-generated list of authorized users. Determine the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed.		
AC-2.3 Owners determine disposition and sharing of data.	Standard forms are used to document approval for archiving, deleting, or sharing data files.	Examine standard approval forms. Interview data owners.		
	Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.	Examine documents authorizing file sharing and file sharing agreements.		

Appendix III

3.2 ACCESS CONTROL (AC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
AC-3 Establish physical and logical controls to prevent or detect unauthorized access.				
AC-3.1 Adequate physical security controls have been implemented.		*These audit procedures should be coordinated with section SC-2.2 (environmental controls) since many of the control objectives and techniques are the same.*		
A. Physical safeguards have been established that are commensurate with the risks of physical damage or access.	Facilities housing sensitive and critical resources have been identified. All significant threats to the physical well-being of sensitive and critical resources have been identified and related risks determined.	Review a diagram of the physical layout of the computer, telecommunications, and cooling system facilities. Walk through facilities. Review risk analysis.		
	Access is limited to those individuals who routinely need access through the use of guards, identification badges, or entry devices, such as key cards. Management regularly reviews the list of persons with physical access to sensitive facilities.	Review lists of individuals authorized access to sensitive areas and determine the appropriateness for access. Before becoming recognized as the auditor, attempt to access sensitive areas without escort or identification badges. Observe entries to and exits from facilities during and after normal business hours. Observe utilities access paths. Interview management.		
	Keys or other access are needed to enter the computer room and tape/media library.	Observe entries to and exits from sensitive areas during and after normal business hours. Interview employees.		

3.2 ACCESS CONTROL (AC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
A. Physical safeguards have been established that are commensurate with the risks of physical damage or access. (continued)	All deposits and withdrawals of tapes and other storage media from the library are authorized and logged.	Review procedures for the removal and return of storage media from and to the library. Select from the log some returns and withdrawals, verify the physical existence of the tape or other media, and determine whether proper authorization was obtained for the movement.		
	Unissued keys or other entry devices are secured.	Observe practices for safeguarding keys and other devices.		
	Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to reenter after fire drills, etc.	Review written emergency procedures. Examine documentation supporting prior fire drills. Observe a fire drill.		
B. Visitors are controlled.	Visitors to sensitive areas, such as the main computer room and tape/media library, are formally signed in and escorted.	Review visitor entry logs. Observe entries to and exits from sensitive areas during and after normal business hours. Interview guards at facility entry.		
	Entry codes are changed periodically.	Review documentation on and logs of entry code changes.		
	Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.	Observe appointment and verification procedures for visitors.		

Appendix III

3.2 ACCESS CONTROL (AC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
AC-3.2 Adequate logical access controls have been implemented.				
A. Passwords, tokens, or other devices are used to identify and authenticate users.	Passwords are • unique for specific individuals, not groups; • controlled by the assigned user and not subject to disclosure; • changed periodically--every 30 to 90 days; • not displayed when entered; • at least 6 alphanumeric characters in length; and • prohibited from reuse for at least 6 generations.	Review pertinent policies and procedures. Interview users. Review security software password parameters. Observe users keying in passwords. Attempt to log on without a valid password; make repeated attempts to guess passwords. Assess procedures for generating and communicating passwords to users.		
	Use of names or words is prohibited.	Review a system-generated list of current passwords. Search password file using audit software.		
	Vendor-supplied passwords are replaced immediately.	Attempt to log on using common vendor supplied passwords. Search password file using audit software.		
	Generic user IDs and passwords are not used.	Interview users and security managers. Review a list of IDs and passwords.		
	Attempts to log on with invalid passwords are limited to 3-4 attempts.	Repeatedly attempt to log on using invalid passwords. Review security logs.		

Appendix III

3.2 ACCESS CONTROL (AC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
A. Passwords, tokens, or other devices are used to identify and authenticate users. (continued)	Personnel files are automatically matched with actual system users to remove terminated or transferred employees from the system.	Review pertinent policies and procedures. Review documentation of such comparisons. Interview security managers. Make comparison using audit software.		
	Password files are encrypted.	View dump of password files (e.g., hexadecimal printout).		
	For other devices, such as tokens or key cards, users • maintain possession of their individual tokens, cards, etc, and • understand that they must not loan or share these with others and must report lost items immediately.	Interview users To evaluate biometrics or other technically sophisticated authentication techniques, the auditor should obtain the assistance of a specialist.		
B. Identification of access paths.	An analysis of the logical access paths is performed whenever system changes are made.	Review access path diagram.		
C. Logical controls over data files and software programs.	Security software is used to restrict access. Access to security software is restricted to security administrators only.	Interview security administrators and system users. Review security software parameters.		
	Computer terminals are automatically logged off after a period of inactivity.	Observe terminals in use. Review security software parameters.		
	Inactive users' accounts are monitored and removed when not needed.	Review security software parameters. Review a system-generated list of inactive logon IDs, and determine why access for these users has not been terminated.		

3.2 ACCESS CONTROL (AC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
C. Logical controls over data files and software programs. (continued)	Security administration personnel set parameters of security software to provide access as authorized and restrict access that has not been authorized. This includes access to data files, load libraries, batch operational procedures, source code libraries, security files, and operating system files. Naming conventions are used for resources.	Determine library names for sensitive or critical files and libraries and obtain security reports of related access rules. Using these reports, determine who has access to critical files and libraries and whether the access matches the level and type of access authorized. Perform penetration testing by attempting to access and browse computer resources including critical data files, production load libraries, batch operational procedures (e.g., JCL libraries), source code libraries, security software, and the operating system. These tests should be performed as (1) an "outsider" with no information about the entity's computer systems; and (2) an "outsider" with prior knowledge about the systems--e.g., an ex-insider, and (3) an "insider" with and without specific information about the entity's computer systems, and with access to the entity's facilities. When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet. When performing insider tests, use an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, try to access the entity's computer resources using default/generic IDs with easily guessed passwords. Determine whether naming conventions are used.		

3.2 ACCESS CONTROL (AC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
D. Logical controls over a database.	Database management systems (DBMS) and data dictionary (DD) controls have been implemented that • restrict access to data files at the logical data view, field, or field-value level; • control access to the DD using security profiles and passwords; • maintain audit trails that allow monitoring of changes to the DD; and • provide inquiry and update capabilities from application program functions, interfacing DBMS or DD facilities	Review pertinent policies and procedures. Interview database administrator. Review DBMS and DD security parameters. Test controls by attempting access to restricted files.		
	Use of DBMS utilities is limited.	Review security system parameters.		
	Access and changes to DBMS software are controlled.			
	Access to security profiles in the DD and security tables in the DBMS is limited.			

Appendix III

3.2 ACCESS CONTROL (AC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
E. Logical controls over telecommunications access.	Communication software has been implemented to • verify terminal identifications in order to restrict access through specific terminals; • verify IDs and passwords for access to specific applications; • control access through connections between systems and terminals; • restrict an application's use of network facilities; • protect sensitive data during transmission; • automatically disconnect at the end of a session; • maintain network activity logs; • restrict access to tables that define network options, resources, and operator profiles; • allow only authorized users to shut down network components; • monitor dial-in access by monitoring the source of calls or by disconnecting and then dialing back at preauthorized phone numbers; • restrict in-house access to telecommunications software; • control changes to telecommunications software; • ensure that data are not accessed or modified by an unauthorized user during transmission or while in temporary storage; and • restrict and monitor access to telecommunications hardware or facilities.	Review pertinent policies and procedures. Review parameters set by communications software or teleprocessing monitors. Test telecommunications controls by attempting to access various files through communications networks. Identify all dial-up lines through automatic dialer software routines and compare with known dial-up access. Discuss discrepancies with management. Interview telecommunications management staff and users.		
	In addition to logical controls: The opening screen viewed by a user provides a warning and states that the system is for authorized use only and that activity will be monitored. Dial-in phone numbers are not published and are periodically changed.	Review pertinent policies and procedures. View the opening screen seen by telecommunication system users. Review documentation showing changes to dial-in numbers. Review entity's telephone directory to verify that the numbers are not listed.		

3.2 ACCESS CONTROL (AC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
AC-3.3 Cryptographic tools.	Cryptographic tools have been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs.	To evaluate cryptographic tools, the auditor should obtain the assistance of a specialist.		
AC-3.4 Sanitation of equipment and media prior to disposal or reuse.	Procedures are implemented to clear sensitive data and software from discarded and transferred equipment and media.	Review written procedures. Interview personnel responsible for clearing equipment and media. For a selection of recently discarded or transferred items, examine documentation related to clearing of data and software. For selected items still in the entity's possession, test that they have been appropriately sanitized.		
AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action.				
AC-4.1 Audit trails are maintained.	All activity involving access to and modifications of sensitive or critical files is logged.	Review security software settings to identify types of activity logged.		
AC-4.2 Actual or attempted unauthorized, unusual, or sensitive access is monitored.	Security violations and activities, including failed logon attempts, other failed access attempts, and sensitive activity, are reported to management and investigated.	Review pertinent policies and procedures. Review security violation reports. Examine documentation showing reviews of questionable activities.		

Appendix III

3.2 ACCESS CONTROL (AC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
AC-4.3 Suspicious access activity is investigated and appropriate action taken.	Security managers investigate security violations and report results to appropriate supervisory and management personnel. Appropriate disciplinary actions are taken.	Test a selection of security violations to verify that follow-up investigations were performed and to determine what action were taken against the perpetrator.		
	Violations are summarized and reported to senior management.	Interview senior management and personnel responsible for summarizing violations. Review any supporting documentation.		
	Access control policies and techniques are modified when violations and related risk assessments indicate that such changes are appropriate.	Review policies and procedures and interview appropriate personnel. Review any supporting documentation.		

3.3 APPLICATION SOFTWARE DEVELOPMENT AND CHANGE CONTROL (CC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
CC-1 Processing features and program modifications are properly authorized.				
CC-1.1 A system development life cycle methodology (SDLC) has been implemented.	A SDLC methodology has been developed that • provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process, • is sufficiently documented to provide guidance to staff with varying levels of skill and experience, • provides a means of controlling changes in requirements that occur over the system's life, and • includes documentation requirements.	Review SDLC methodology. Review system documentation to verify that SDLC methodology was followed.		
	Program staff and staff involved in developing and testing software have been trained and are familiar with the use of the organization's SDLC methodology	Interview staff. Review training records.		
CC-1.2 Authorizations for software modifications are documented and maintained.	Software change request forms are used to document requests and related approvals. Change requests must be approved by both system users and data processing staff.	Identify recent software modifications and determine whether change request forms were used. Examine a selection of software change request forms for approvals. Interview software development staff.		
CC-1.3 Use of public domain and personal software is restricted.	Clear policies restricting the use of personal and public domain software have been developed and are enforced. The entity uses virus identification software.	Review pertinent policies and procedures Interview users and data processing staff.		

3.3 APPLICATION SOFTWARE DEVELOPMENT AND CHANGE CONTROL (CC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
CC-2 Test and approve all new and revised software.				
CC-2.1 Changes are controlled as programs progress through testing to final approval.	Test plan standards have been developed for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, library control).	Review test plan standards.		
	Detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.	For the software change requests selected for control activity CC-1.2: • review specifications; • trace changes from code to design specifications; • review test plans; • compare test documentation with related test plans; • analyze test failures to determine if they indicate ineffective software testing; • review test transactions and data;		
	Software changes are documented so that they can be traced from authorization to the final approved code and they facilitate "trace-back" of code to design specifications and functional requirements by system testers.			
	Test plans are documented and approved that define responsibilities for each party involved (e.g., users, systems analysts, programmers, auditors, quality assurance, library control).			
	Unit, integration, and system testing are performed and approved • in accordance with the test plan and • applying a sufficient range of valid and invalid conditions.			
	A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing. Live data are not used in testing of program changes, except to build test data files.			

3.3 APPLICATION SOFTWARE DEVELOPMENT AND CHANGE CONTROL (CC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
CC-2.1 Changes are controlled as programs progress through testing to final approval. (continued)	Test results are reviewed and documented.	For the software change requests selected for control activity CC-1.2 (continued): • review test results; • review documentation of management or security administrator reviews; • verify user acceptance; and • review updated documentation. Determine whether operational systems experience a high number of abends and, if so, whether they indicate inadequate testing prior to implementation.		
	Program changes are moved into production only upon documented approval from users and system development management.			
	Documentation is updated for software, hardware, operating personnel, and system users when a new or modified system is implemented.			
	Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.			
CC-2.2 Emergency changes are promptly tested and approved.	Emergency change procedures are documented.	Review procedures.		
	Emergency changes are documented and • approved by the operations supervisor, • formally reported to computer operations management for follow-up, and • approved after the fact by programming supervisors and user management.	For a selection of emergency changes recorded in the emergency change log, review related documentation and approval.		
CC-2.3 Distribution and implementation of new or revised software is controlled.	Standardized procedures are used to distribute new software for implementation.	Examine procedures for distributing new software.		
	Implementation orders, including effective date, are provided to all locations where they are maintained on file.	Examine implementation orders for a sample of changes.		

3.3 APPLICATION SOFTWARE DEVELOPMENT AND CHANGE CONTROL (CC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
CC-3 Control software libraries.				
CC-3.1 Programs are labeled and inventoried.	Library management software is used to • produce audit trails of program changes, • maintain program version numbers, • record and report program changes, • maintain creation/date information for production modules, • maintain copies of previous versions, and • control concurrent updates.	Review pertinent policies and procedures. Interview personnel responsible for library control. Examine a selection of programs maintained in the library and assess compliance with prescribed procedures. Determine how many prior versions of software modules are maintained.		
CC-3.2 Access to program libraries is restricted.	Separate libraries are maintained for program development and maintenance, testing, and production programs.	Examine libraries in use. Interview library control personnel.		
	Source code is maintained in a separate library.	Examine libraries in use. Verify that source code exists for a selection of production load modules by (1) comparing compile dates, (2) recompiling the source modules, and (3) comparing the resulting module size to production load modules size.		
	Access to all programs, including production code, source code, and extra program copies, are protected by access control software and operating system features.	For critical software production programs, determine whether access control software rules are clearly defined. Test access to program libraries by examining security system parameters.		
	All deposits and withdrawals of program tapes to/from the tape library are authorized and logged.	Select some program tapes from the log and verify the existence of the tapes either in the library or with the individual responsible for withdrawing the tapes.		

3.3 APPLICATION SOFTWARE DEVELOPMENT AND CHANGE CONTROL (CC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
CC-3.3 Movement of programs and data among libraries is controlled.	A group independent of the user and programmers controls movement of programs and data among libraries. Before and after images of program code are maintained and compared to ensure that only approved changes are made.	Review pertinent policies and procedures. For a selection of program changes, examine related documentation to verify that • procedures for authorizing movement among libraries were followed and • before and after images were compared.		

3.4 SYSTEM SOFTWARE (SS)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SS-1 Limit access to system software.				
SS-1.1 Access authorizations are appropriately limited.	Policies and procedures for restricting access to systems software exist and are up-to-date.	Review pertinent policies and procedures. Interview management and systems personnel regarding access restrictions. Observe personnel accessing system software, such as sensitive utilities, and note the controls encountered to gain access. Attempt to access the operating system and other system software.		
	Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. Application programmers and computer operators are specifically prohibited from accessing system software.			
	Documentation showing justification and management approval for access to system software is kept on file.	Select some systems programmers and determine whether management-approved documentation supports their access to system software. Select some application programmers and determine whether they are not authorized access.		
	The access capabilities of system programmers are periodically reviewed for propriety to see that access permissions correspond with job duties.	Determine the last time the access capabilities of system programmers were reviewed.		

3.4 SYSTEM SOFTWARE (SS)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths.	The operating system is configured to prevent circumvention of the security software and application controls.	Test the operating system parameters to verify that it is configured to maintain the integrity of the security software and application controls. (The specifics of this step will be determined by the operating system in use. The auditor should consult audit guides for the operating system in use. This step may be facilitated by use of CA-EXAMINE, the DEC VAX Toolkit, or other audit tools. However, the auditor should be experienced in using the specific software tool, or seek the assistance of someone who is.)		
		Obtain a list of vendor-supplied software and determine if any of these products have known deficiencies that adversely impact the operating system integrity controls. Judgmentally review the installation of system software components and determine whether they were appropriately installed to preclude adversely impacting operating system integrity controls.		

3.4 SYSTEM SOFTWARE (SS)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths. (continued)	The operating system is configured to prevent circumvention of the security software and application controls. (continued)	Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods including: •Determine whether the operating system's subsystems have been appropriately implemented to ensure that they support integrity controls. (For example, with MVS, the auditor should evaluate IPL controls; APF update controls and implementation of key MVS libraries and locally defined and tailored system libraries; SVC controls, including imbedded passwords and controls to prevent interception; SMF options; and PPT.) •Determine whether applications interfaces have been implemented to support operating system integrity controls, including on-line transaction monitors; database software; on-line editors; on-line direct-access storage devices; on-line operating system datasets; exits related to the operating system, security, and program products; and controls over batch processing, to include security controls, scheduler controls, and access authorities. (For example, with MVS, the evaluated interfaces should include CICS, ADABAS, IMS, IDMS, TSO and/or similar packages; on-line DASD volumes; and on-line MVS datasets, such as CLIST, PARMLIB, SPOOL, DUMP, and TRACE, I/O appendages, and JES2/JES3.)		

3.4 SYSTEM SOFTWARE (SS)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths. (continued)	The operating system is configured to prevent circumvention of the security software and application controls. (continued)	Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods including: (continued) •Evaluate the controls over external access to computer resources including networks, dial-up, LAN, WAN, RJE, and the Internet. •Identify potential opportunities to adversely impact the operating system and its products through trojan horses, viruses, and other malicious actions.		
	Access to system software is restricted to personnel with corresponding job responsibilities by access control software. Update access should generally be limited to primary and backup systems programmers. All accesses to system software files are logged by automated logging facilities.	Obtain a list of all system software on test and production libraries used by the entity. Verify that access control software restricts access to system software. Using security software reports, determine who has access to system software files, security software, and logging files. Preferably, reports should be generated by the auditor, but at a minimum, they should be generated in the presence of the auditor. Verify that system programmer's access to production data and programs is only allowed under controlled updates and during emergencies when established procedures are followed.		

Appendix III

3.4 SYSTEM SOFTWARE (SS)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths. (continued)	Vendor-supplied default logon IDs and passwords have been disabled.	Inquire whether disabling has occurred. Test for default presence using vendor standard IDs and passwords.		
	Remote access to the system master console is restricted. Physical and logical controls provide security over all terminals that are set up as master consoles.	Determine what terminals are set up as master consoles and what controls exist over them. Test to determine if the master console can be accessed or if other terminals can used to mimic the master console and take control of the system.		
SS-2 Monitor access to and use of system software.				
SS-2.1 Policies and techniques have been implemented for using and monitoring use of system utilities.	Policies and procedures for using and monitoring use of system software utilities exist and are up-to-date.	Review pertinent policies and procedures. Interview management and systems personnel regarding their responsibilities.		
	Responsibilities for using sensitive system utilities have been clearly defined and are understood by systems programmers.			
	Responsibilities for monitoring use are defined and understood by technical management.			
	The use of sensitive system utilities is logged using access control software reports or job accounting data (e.g., IBM's System Management Facility).	Determine whether logging occurs and what information is logged. Review logs. Using security software reports, determine who can access the logging files.		
SS-2.2 Inappropriate or unusual activity is investigated and appropriate actions taken.	The use of privileged system software and utilities is reviewed by technical management.	Interview technical management regarding their reviews of privileged system software and utilities usage. Review documentation supporting their reviews.		

3.4 SYSTEM SOFTWARE (SS)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SS-2.2 Inappropriate or unusual activity is investigated and appropriate actions taken. (continued)	Inappropriate or unusual activity in using utilities is investigated.	Interview management and systems personnel regarding these investigations. Review documentation supporting these investigations.		
	System programmers' activities are monitored and reviewed.	Interview systems programmer supervisors to determine their activities related to supervising and monitoring their staff. Review documentation supporting their supervising and monitoring of systems programmers' activities		
	Management reviews are performed to determine that control techniques for monitoring use of sensitive system software are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).	Interview management and analyze their reviews concerning the use of system software. Determine what management reviews have been conducted, and their currency, over this area.		
SS-3 Control system software changes.				
SS-3.1 System software changes are authorized, tested, and approved before implementation.	Polices and procedures exist and are up-to-date for identifying, selecting, installing, and modifying system software. Procedures include an analysis of costs and benefits and consideration of the impact on processing reliability and security.	Review pertinent policies and procedures. Interview management and systems personnel.		
	Procedures exist for identifying and documenting system software problems. This should include using a log to record the problem, the name of the individual assigned to analyze the problem, and how the problem was resolved.	Review procedures for identifying and documenting system software problems. Interview management and systems programmers. Review the causes and frequency of any recurring system software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems.		

3.4 SYSTEM SOFTWARE (SS)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SS-3.1 System software changes are authorized, tested, and approved before implementation. (continued)	New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document.	Determine what authorizations and documentation are required prior to initiating system software changes. Select recent system software changes and determine whether the authorization was obtained and the change is supported by a change request document.		
	New system software versions or products and modifications to existing system software are tested and the test results are approved before implementation. Procedures include: • a written standard that guides the testing, which is conducted in a test rather than production environment; • specification of the optional security-related features to be turned on, when appropriate; • review of test results by technically qualified staff who document their opinion on whether the system software is ready for production use; and • review of test results and documented opinions by data center management prior to granting approval to move the system software into production use.	Determine the procedures used to test and approve system software prior to its implementation. Select recent system software changes and test whether the indicated procedures were in fact used.		
	Procedures exist for controlling emergency changes. Procedures include: • authorizing and documenting emergency changes as they occur; • reporting the changes for management review; and • review by an independent IS supervisor of the change.	Review procedures used to control and approve emergency changes. Select some emergency changes to system software and test whether the indicated procedures were in fact used.		

3.4 SYSTEM SOFTWARE (SS)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SS-3.2 Installation of system software is documented and reviewed.	Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.	Interview management and systems programmers about scheduling and giving advance notices when system software is installed. Review recent installations and determine whether scheduling and advance notification did occur. Determine whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.		
	Migration of tested and approved system software to production use is performed by an independent library control group. Outdated versions of system software are removed from production libraries.	Interview management, systems programmers, and library control personnel, and determine who migrates approved system software to production libraries and whether outdated versions are removed from production libraries. Review supporting documentation for some system software migrations and the removal of outdated versions from production libraries.		
	Installation of all system software is logged to establish an audit trail and reviewed by data center management.	Interview data center management about their role in reviewing system software installations. Review some recent system software installations and determine whether documentation shows that logging and management review occurred.		

3.4 SYSTEM SOFTWARE (SS)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SS-3.2 Installation of system software is documented and reviewed. (continued)	Vendor-supplied system software is still supported by the vendor.	Interview system software personnel concerning a selection of system software and determine the extent to which the operating version of the system software is currently supported by the vendor.		
	All system software is current and has current and complete documentation.	Interview management and systems programmers about the currency of system software and the currency and completeness of software documentation. Review documentation and test whether recent changes are incorporated.		

3.5 SEGREGATION OF DUTIES (SD)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SD-1 Segregate incompatible duties and establish related policies.				
SD-1.1 Incompatible duties have been identified and policies implemented to segregate these duties.	Policies and procedures for segregating duties exist and are up-to-date.	Review pertinent policies and procedures. Interview selected management and IS personnel regarding segregation of duties.		
	Distinct systems support functions are performed by different individuals, including the following: • IS management. • System design. • Application programming. • Systems programming. • Quality assurance/testing. • Library management/change management. • Computer operations. • Production control and scheduling. • Data control. • Data security. • Data administration. • Network Administration.	Review an agency organization chart showing IS functions and assigned personnel. Interview selected personnel and determine whether functions are appropriately segregated. Determine whether the chart is current and each function is staffed by different individuals. Review relevant alternate or backup assignments and determine whether the proper segregation of duties is maintained. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.		

Appendix III

3.5 SEGREGATION OF DUTIES (SD)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SD-1.1 Incompatible duties have been identified and policies implemented to segregate these duties. (continued)	No individual has complete control over incompatible transaction processing functions. Specifically, the following combination of functions are not performed by a single individual: • Data entry and verification of data. • Data entry and its reconciliation to output. • Input of transactions for incompatible processing functions (e.g., input of vendor invoices and purchasing and receiving information). • Data entry and supervisory authorization functions (e.g., authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's review and approval).	Review the organizational chart and interview personnel to determine that assignments do not result in a single person being responsible for the indicated combinations of functions. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.		
	Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.	Interview management, observe activities, and test transactions. *Note: Perform this in conjunction with SD-3.2.*		
	Data processing personnel are not users of information systems. They and security managers do not initiate, input, or correct transactions .	Determine through interview and observation whether data processing personnel and security managers are prohibited from these activities.		
	Day-to-day operating procedures for the data center are adequately documented and prohibited actions are identified.	Review the adequacy of documented operating procedures for the data center.		
	Regularly scheduled vacations and periodic job/shift rotations are required (see SP-4.1 on personnel policies).	*Audit procedures are found in section SP-4.1, but this item is listed here as a reminder. Individuals performing incompatible duties and acting inappropriately could be detected when another individual undertakes those duties. Requiring vacations and rotations helps detect such actions.*		

Appendix III

3.5 SEGREGATION OF DUTIES (SD)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SD-1.2 Job descriptions have been documented.	Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.	Review job descriptions for several positions in organizational units and for user security administrators. Determine whether duties are clearly described and prohibited activities are addressed. Review the effective dates of the position descriptions and determine whether they are current. Compare these descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.		
	Documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and can be used for hiring, promoting, and performance evaluation purposes.	Review job descriptions and interview management personnel.		
SD-1.3 Employees understand their duties and responsibilities.	All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.	Interview personnel filling positions for the selected job descriptions (see above). Determine if the descriptions match their understanding of their duties and responsibilities and whether additional duties are undertaken that are not listed in their job descriptions.		
	Senior management is responsible for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization.	Determine from interviewed personnel whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.		
	Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood, and followed.	Interview management personnel in these activities.		

Appendix III

3.5 SEGREGATION OF DUTIES (SD)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SD-2 Establish access controls to enforce segregation of duties.				
SD-2.1 Physical and logical access controls have been established.	Physical and logical access controls help restrict employees to authorized actions based upon organizational and individual job responsibilities.	Interview management and subordinate personnel. *Note: This audit step should be performed in conjunction with audit steps in section AC-3..*		
SD-2.2 Management reviews effectiveness of control techniques.	Staff's performance should be monitored on a periodic basis and controlled to ensure that objectives laid out in job descriptions are carried out.	Interview management and subordinate personnel. Select documents or actions requiring supervisory review and approval for evidence of such performance (e.g., approval of input of transactions, software changes).		
	Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).	Determine which reviews are conducted to assess the adequacy of duty segregation. Obtain and review results of such reviews. *Note: This audit step should be performed in conjunction with audit steps in critical elements SP-1 and SP-5.*		

Appendix III

3.5 SEGREGATION OF DUTIES (SD)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SD-3 Control personnel activities through formal operating procedures and supervision and review.				
SD-3.1 Formal procedures guide personnel in performing their duties.	Detailed, written instructions exist and are followed for the performance of work.	Review manuals. Interview supervisors and personnel. Observe processing activities.		
	Operator instruction manuals provide guidance on system operation.			
	Application run manuals provide instruction on operating specific applications.			
	Operators are prevented from overriding file label or equipment error messages.			
SD-3.2 Active supervision and review are provided for all personnel.	Personnel are provided adequate supervision and review, including each shift for computer operations.	Interview supervisors and personnel Observe processing activities. Review history log reports for signatures indicating supervisory review. Determine who is authorized to perform the initial program load for the system, what steps are followed, and what controls are in place to monitor console activity during the process. Determine whether operators override the IPL parameters.		
	All operator activities on the computer system are recorded on an automated history log.			
	Supervisors routinely review the history log and investigate any abnormalities.			
	System startup is monitored and performed by authorized personnel. Parameters set during the initial program load (IPL) are in accordance with established procedures.			

Appendix III

3.6 SERVICE CONTINUITY (SC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources.				
SC-1.1 Critical data and operations are identified and prioritized.	A list of critical operations and data has been documented that • prioritizes data and operations, • is approved by senior program managers, and • reflects current conditions.	Review related policies. Review list and any related documentation. Interview program, data processing, and security administration officials. Determine their input and their assessment of the reasonableness of priorities established.		
SC-1.2 Resources supporting critical operations are identified.	Resources supporting critical operations have been identified and documented. Types of resources identified should include • computer hardware, • computer software, • computer supplies, • system documentation, • telecommunications, • office facilities and supplies, and • human resources.	Review related documentation. Interview program and security administration officials.		
SC-1.3 Emergency processing priorities are established.	Emergency processing priorities have been documented and approved by appropriate program and data processing managers.	Review related policies. Review related documentation. Interview program and security administration officials.		

Appendix III

3.6 SERVICE CONTINUITY (SC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SC-2 Take steps to prevent and minimize potential damage and interruption.				
SC-2.1 Data and program backup procedures have been implemented.	Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.	Review written policies and procedures for backing up files. Compare inventory records with the files maintained off-site and determine the age of these files. For a selection of critical files, locate and examine the backup files. Verify that backup files can be used to recreate current reports. Determine whether backup files are created and rotated off-site as prescribed and are sent before prior versions are returned.		
	System and application documentation are maintained at the off-site storage location.	Locate and examine documentation.		
	The backup storage site is • geographically removed from the primary site(s), and • protected by environmental controls and physical access controls.	Examine the backup storage site.		

Appendix III

3.6 SERVICE CONTINUITY (SC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SC-2.2 Adequate environmental controls have been implemented.		*These procedure should be performed in conjunction with Section AC-3.3, regarding physical access controls.*		
	Fire suppression and prevention devices have been installed and are working, e.g., smoke detectors, fire extinguishers, and sprinkler systems. Controls have been implemented to mitigate other disasters, such as floods, earthquakes, etc. Redundancy exists in the air cooling system. Building plumbing lines do not endanger the computer facility or, at a minimum, shut-off valves and procedures exist and are known. An uninterruptible power supply or backup generator has been provided so that power will be adequate for orderly shut down.	Examine the entity's facilities. Interview site managers. Observe that operations staff are aware of the locations of fire alarms, fire extinguishers, regular and auxiliary electrical power switches, water shut-off valves, breathing apparatus, and other devices that they may be expected to use in an emergency. Observe the operation, location, maintenance and access to the air cooling systems. Observe whether water can enter through the computer room ceiling or pipes are running through the facility and that there are water detectors on the floor. Determine whether the activation of heat and smoke detectors will notify the fire department.		
	Environmental controls are periodically tested.	Review test policies. Review documentation supporting recent tests of environmental controls.		
	Eating, drinking, and other behavior that may damage computer equipment is prohibited.	Review policies and procedures regarding employee behavior. Observe employee behavior.		

Appendix III

3.6 SERVICE CONTINUITY (SC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SC-2.3 Staff have been trained to respond to emergencies.	All data center employees have received training and understand their emergency roles and responsibilities. Data center staff receive periodic training in emergency fire, water, and alarm incident procedures. Emergency response procedures are documented.	Interview data center staff. Review training records Review training course documentation. Review emergency response procedures.		
	Emergency procedures are periodically tested.	Review test policies. Review test documentation. Interview data center staff.		
SC-2.4 Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	Policies and procedures exist and are up-to-date.	Review policies and procedures.		
	Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations.	Interview data processing and user management. Review maintenance documentation.		
	Regular and unscheduled maintenance performed is documented.			
	Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled maintenance.			
	Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.	Interview data center management.		
	Goals are established by senior management on the availability of data processing and on-line services.	Interview senior management, data processing management, and user management. Review supporting documentation.		
	Records are maintained on the actual performance in meeting service schedules.			

Appendix III

3.6 SERVICE CONTINUITY (SC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SC-2.4 Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions. (continued)	Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.	Interview senior management, data processing management, and user management. Review supporting documentation.		
	Senior management periodically reviews and compares the service performance achieved with the goals and surveys user departments to see if their needs are being met.			
	Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing.			
	Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.			

Appendix III

3.6 SERVICE CONTINUITY (SC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SC-3 Develop and document a comprehensive contingency plan.				
SC-3.1 An up-to-date contingency plan is documented.	A contingency plan has been documented that • reflects current conditions, • has been approved by key affected groups including senior management, data center management, and program managers, • clearly assigns responsibilities for recovery, • includes detailed instructions for restoring operations (both operating system and critical applications), • identifies the alternate processing facility and the backup storage facility, • includes procedures to follow when the data/service center is unable to receive or transmit data, • identifies critical data files, • is detailed enough to be understood by all agency managers, • includes computer and telecommunications hardware compatible with the agencies needs, and • has been distributed to all appropriate personnel.	Review the contingency plan and compare its provisions with the most recent risk assessment and with a current description of automated operations. Interview senior management, data center management, and program managers.		
	The plan provides for backup personnel so that it can be implemented independent of specific individuals. User departments have developed adequate manual/peripheral processing procedures for use until operations are restored.	Review the contingency plan. Interview senior management, data center management, and program managers.		

Appendix III

3.6 SERVICE CONTINUITY (SC)

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SC-3.1 An up-to-date contingency plan is documented. (continued)	Several copies of the current contingency plan are securely stored off-site at different locations.	Observe copies of the contingency plan held off-site.		
	The contingency plan is periodically reassessed and, if appropriate, revised to reflect changes in hardware, software, and personnel	Review the plan and any documentation supporting recent plan reassessments.		
SC-3.2 Arrangements have been made for alternate data processing and telecommunications facilities.	Contracts or interagency agreements have been established for a backup data center and other needed facilities that • are in a state of readiness commensurate with the risks of interrupted operations, • have sufficient processing capacity, and • are likely to be available for use. Alternate telecommunication services have been arranged. Arrangements are planned for travel and lodging of necessary personnel, if needed.	Review contracts and agreements.		
SC-4 Periodically test the contingency plan and adjust it as appropriate.				
SC-4.1 The plan is periodically tested.	The current plan has been tested under conditions that simulate a disaster.	Review policies on testing. Review test results. Observe a disaster recovery test.		
SC-4.2 Test results are analyzed and contingency plans are adjusted accordingly.	Test results were documented and a report, such as a "lessons learned" report, was developed and provided to senior management.	Review final test report. Interview senior managers to determine if they are aware of the test results.		
	The contingency plan and related agreements and preparations were adjusted to correct any deficiencies identified during testing.	Review any documentation supporting contingency plan adjustments.		

[This page intentially left blank.]

Appendix IV

TABLES FOR ASSESSING THE EFFECTIVENESS OF GENERAL CONTROLS

The tables in this appendix are provided for the auditor's use in recording the control effectiveness for each critical element in each general control category, as well as formulating an overall assessment of each general control category. Judging control effectiveness should be based on the results of audit work performed and assessments of control effectiveness for specific control techniques, as summarized in Appendix III. After completing Appendix IV, the auditor should prepare a narrative summarizing the control effectiveness for general controls. This narrative should also state whether or not audit work should be conducted to determine the reliability of application controls. These tables are available in electronic form from GAO's World Wide Web server. Our Internet address is: **<http://www.gao.gov>**.

3.1 ENTITYWIDE SECURITY PROGRAM PLANNING AND MANAGEMENT (SP)

Critical Elements	Are Controls Effective?			Comments on Control Effectiveness	Work Paper References
	Yes	No	Partially		
SP-1 Periodically assess risks					
SP-2 Document an entitywide security program plan					
SP-3 Establish a security management structure and clearly assign security responsibilities					
SP-4 Implement effective security-related personnel policies					
SP-5 Monitor the security program's effectiveness and make changes as needed					
Overall assessment of entitywide security program planning and management					

3.2 ACCESS CONTROL (AC)

Critical Elements	Are Controls Effective?			Comments on Control Effectiveness	Work Paper References
	Yes	No	Partially		
AC-1 Classify information resources according to their criticality and sensitivity					
AC-2 Maintain a current list of authorized users and their access authorized					
AC-3 Establish physical and logical controls to prevent or detect unauthorized access					
AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action.					
Overall assessment of access controls					

3.3 APPLICATION SOFTWARE DEVELOPMENT AND CHANGE CONTROL (CC)

Critical Elements	Are Controls Effective?			Comments on Control Effectiveness	Work Paper References
	Yes	No	Partially		
CC-1 Processing features and program modifications are properly authorized					
CC-2 Test and approve all new and revised software					
CC-3 Control software libraries					
Overall assessment of application software development and change control					

3.4 SYSTEM SOFTWARE (SS)

Critical Elements	Are Controls Effective?			Comments on Control Effectiveness	Work Paper References
	Yes	No	Partially		
SS-1 Limit access to system software					
SS-2 Monitor access to and use of system software					
SS-3 Control system software changes					
Overall assessment of system software					

Appendix IV

3.5 SEGREGATION OF DUTIES (SD)

Critical Elements	Are Controls Effective?			Comments on Control Effectiveness	Work Paper References
	Yes	No	Partially		
SD-1 Segregate incompatible duties and establish related policies					
SD-2 Establish access controls to enforce segregation of duties					
SD-3 Control personnel activities through formal operating procedures and supervision and review					
Overall assessment of segregation of duties					

Appendix IV

3.6 SERVICE CONTINUITY (SC)

Critical Elements	Are Controls Effective?			Comments on Control Effectiveness	Work Paper References
	Yes	No	Partially		
SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources					
SC-2 Take steps to prevent and minimize potential damage and interruption					
SC-3 Develop and document a comprehensive contingency plan					
SC-4 Periodically test the contingency plan and adjust it as appropriate					
Overall assessment of service continuity					

[This page intentionally left blank.]

Appendix V

KNOWLEDGE, SKILLS, AND ABILITIES NEEDED TO PERFORM AUDIT PROCEDURES IN A COMPUTER-BASED ENVIRONMENT

Generally Accepted Government Auditing Standards (GAGAS) state that the "staff assigned to conduct the audit should collectively possess adequate professional proficiency for the tasks required." The standards further require that, if the work involves a review of computerized systems, the team should include persons with computer audit skills.[1] This appendix provides an overview of the knowledge, skills, and abilities that are needed to effectively perform audit procedures in a computer-based environment for a financial statement audit. It assumes a level of proficiency to perform basic auditing tasks, such as interviewing, evidence gathering and documenting, communicating both orally and in writing, and project management. It focuses on attributes associated with computer auditing. Each staff member assigned to such an audit need not have all of these requisite attributes. However, the audit team must collectively possess the requisite attributes in order to adequately plan the audit, assess the computer-related controls, test the controls, determine the effect on the overall audit plan, develop findings and recommendations, and report the results. The knowledge, skills, and abilities are addressed in accordance with FISCAM's organization. Entities should contract for audit services to perform the audit procedures in areas where in-house staff lack the requisite attributes.

Knowledge, skills, and abilities are typically used in job position descriptions and job announcements where they are defined as follows:

> Knowledge is the foundation upon which skills and abilities are built. Knowledge is an organized body of information, facts, principles, or procedures which, if applied, makes adequate performance of a job possible. An example is knowledge of tools and techniques used to establish logical access control over an information system.
>
> A skill is the proficient manual, verbal, or mental manipulation of people, ideas, or things. A skill is demonstrable and implies a degree of proficiency. As an example a person may be skilled in operating a personal computer to prepare electronic spreadsheets, or in using a software product to conduct an automated review of the integrity of an operating system.
>
> An ability is the power to perform a job function while applying or using the essential knowledge. Abilities are evidenced through activities or behaviors

[1] Government Auditing Standards: 1994 Revision (GAO/OCG-94-4), Paragraphs 3.3 - 3.5, and 3.10.

required to do a job. An example is the ability to apply knowledge about logical access controls to evaluate the adequacy of an entity's implementation of logical access controls.

Entitywide Security Program Planning and Management

- Knowledge of the legislative and federal requirements for an agency security program
- Knowledge of the sensitivity of data and the risk management process through risk assessment and risk mitigation
- Knowledge of the risks associated with a deficient security program
- Knowledge of the elements of a good security program
- Ability to analyze and evaluate an entity's security policies and procedures and identify their strengths and weaknesses

Access Control

- Knowledge across platforms on the access paths into computer systems and on the functions of associated hardware and software providing an access path
- Knowledge on access level privileges granted to users and the technology used to provide and control them
- Knowledge of the procedures, tools, and techniques that provide for good physical, technical, and administrative controls over access
- Knowledge of the risks associated with inadequate access controls
- Ability to analyze and evaluate an entity's access controls and identify the strengths and weaknesses
- Skills to review security software reports and identify access control weaknesses
- Skills to perform penetration testing of the entity's applications and supporting computer systems

Application Software Development and Change Control

- Knowledge of the concept of a system life cycle and of the System Development Life Cycle (SDLC) process
- Knowledge of the auditor's role during system development and of federal guidelines for designing controls into systems during development
- Knowledge of the procedures, tools, and techniques that provide control over application software development and modification
- Knowledge of the risks associated with the development and modification of application software
- Ability to analyze and evaluate the entity's methodology and procedures for system development and modification and identify the strengths and weaknesses

System Software

- Knowledge of the different types of system software and their functions
- Knowledge of the risks associated with system software
- Knowledge of the procedures, tools, and techniques that provide control over the implementation, modification, and use of system software
- Ability to analyze and evaluate an entity's system software controls and identify the strengths and weaknesses
- Skills to use software products to review system software integrity

Segregation of Duties

- Knowledge of the different functions involved with information systems and data processing and incompatible duties associated with these functions
- Knowledge of the risks associated with inadequate segregation of duties
- Ability to analyze and evaluate an entity's organizational structure and segregation of duties and identify the strengths and weaknesses

Service Continuity

- Knowledge of the procedures, tools, and techniques that provide for service continuity
- Knowledge of the risks that exist when measures are not taken to provide for service continuity
- Ability to analyze and evaluate an entity's program and plans for service continuity and identify the strengths and weaknesses

Application Controls

- Knowledge about the practices, procedures, and techniques that provide for the authorization, completeness, and accuracy of application data
- Knowledge of typical applications in each business transaction cycle
- Ability to analyze and evaluate an entity's application controls and identify the strengths and weaknesses
- Skills in flowcharting
- Skills to use a generalized audit software package to conduct data analyses and tests of application data, and to plan, extract, and evaluate data samples

[This page intentionally left blank.]

AUDIT PLANNING STRATEGY: SCOPING THE COMPUTER CONTROL ACTIVITIES AND APPLICATIONS TO REVIEW

This appendix provides a framework for developing a strategy to perform computer control reviews in support of financial statement audits. Reviewing all of an entity's computer control activities each year, including all computerized financial applications, and performing all of the suggested audit procedures in this audit manual, may require more time and audit staff resources than available. Therefore, a strategy is essential to scope the work to be done that provides a means to accomplish the work within a reasonable expenditure of resources, but is sufficient to meet professional standards.

Pages VI-2 and VI-3 provide an overview of the steps involved in assessing the computer related controls. As will be discussed, these steps include scoping the work to be done. In addition, applying the concepts of materiality and rotational and multiple-location auditing can effectively reduce audit requirements, and contracting for audit services can leverage an entity's existing audit staff.

VI.1 STEPS IN ASSESSING COMPUTER RELATED CONTROLS INCLUDE SCOPING DECISIONS

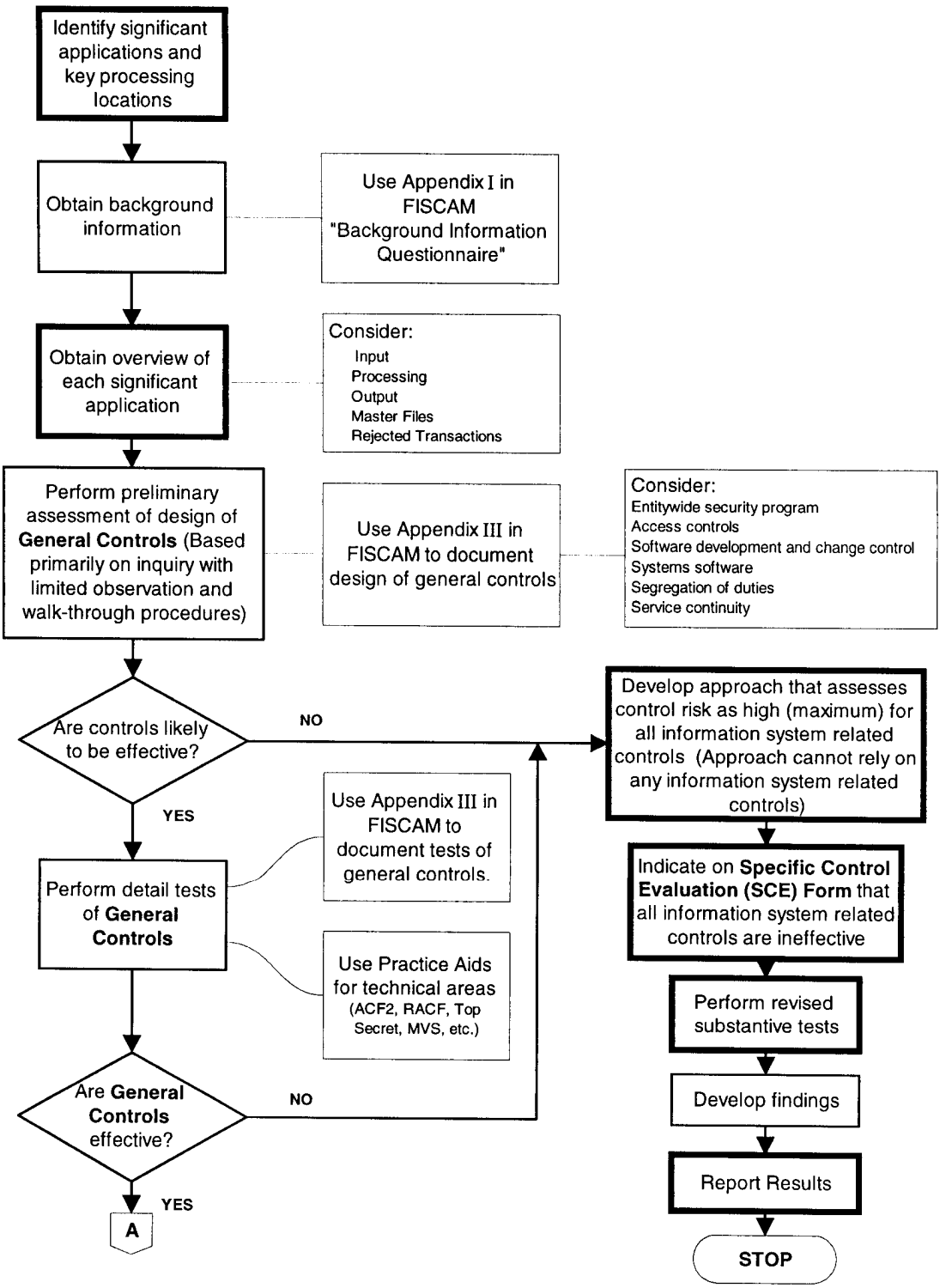
During the planning phase of the audit, the auditor gains an understanding of the entity's operations and identifies significant computer related operations (See section **2.1** of this manual). This is represented by the first three boxes on page VI-2 and includes using **Appendix I** of this manual to obtain background information. The General Section of **Appendix I** provides for gathering relevant GAO, IG, and other reports or studies that may identify existing weaknesses with the entity's information systems. Knowing this information could help avoid control evaluation work when previous efforts have already established that controls are unreliable. Conversely, recent work that has identified control strengths may reduce the level of work needed by the auditors.

VI.1.1 Identify computer applications significant to the financial statements

Responsibility rests with the financial auditor to identify line items and accounts that are significant to the financial statements. The financial auditor, with assistance from an information system auditor, identifies which of these line items and accounts are supported by computer applications. In this regard, the financial auditor prepares an entity profile to compile key data about the agency being audited. In completing the profile, the auditor develops and documents a high-level understanding of the entity's use of computer applications and how they affect the generation of financial statement information. Key sections of the profile include an overview of the entity's computer environment, including descriptions of each of the key computerized financial applications. The profile also includes the operational location of each application, the

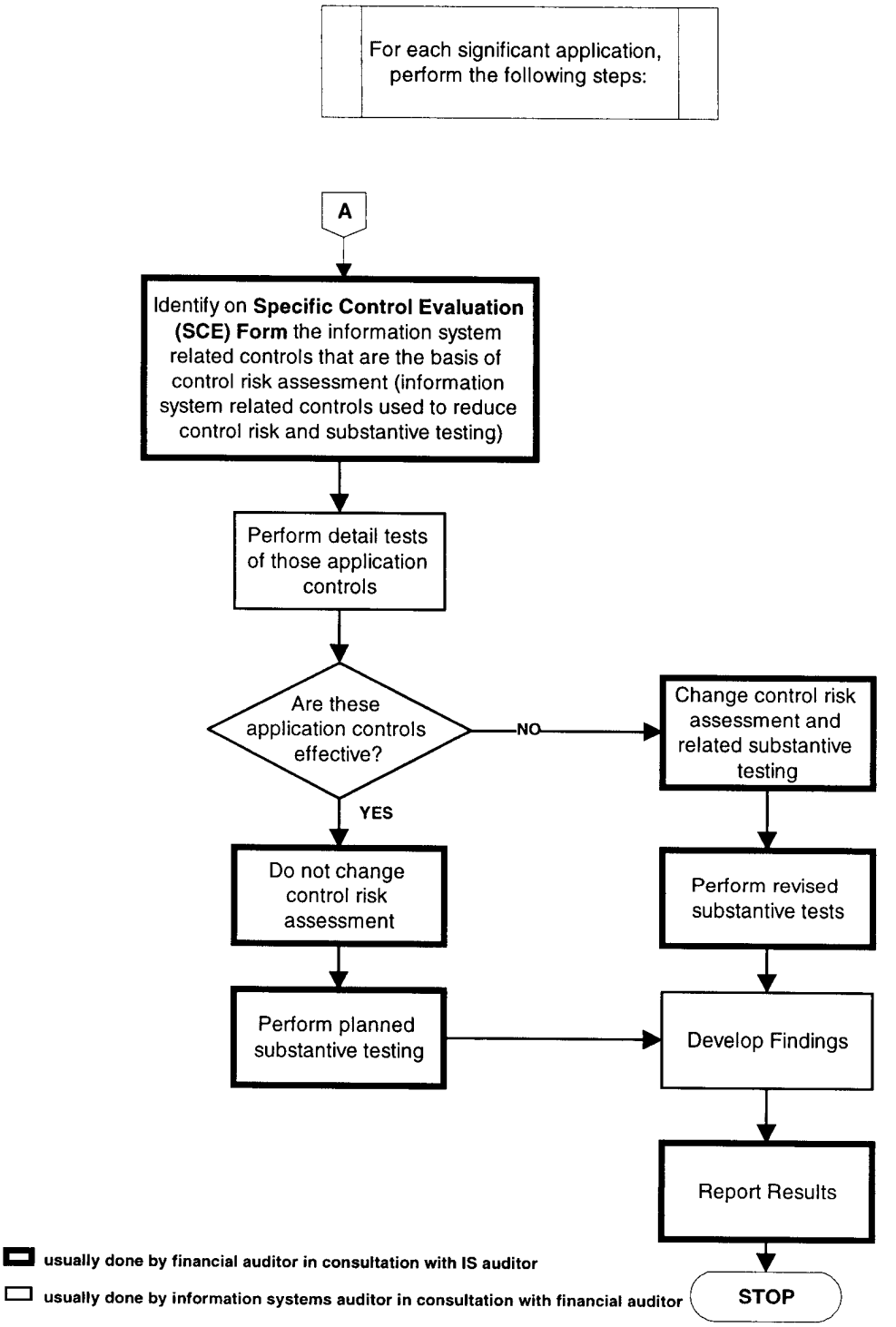
Appendix VI

Steps in Assessing Information System Controls In a Financial Statement Audit



Appendix VI

Steps in Assessing Information System Controls In a Financial Statement Audit -- (continued)



associated hardware and software, and prior audit problems reported. **Appendix I** should be used to help gather this information, and for the most part, can be filled out by representatives of the entity. By identifying the computer applications that are significant to the financial statements, the auditor can concentrate efforts on those applications, and do no or little work associated with the insignificant applications. The applications should be prioritized in order of importance to the financial statements, which may be characterized by the dollar value of the transactions processed, key edits or other controls performed by the application, or summary level reporting of the entity's operations generated by the application.

Identifying the significant computer applications and determining their processing locations and specific environment is a key factor to scoping the necessary computer control evaluation work. As an example, in some cases mainframe computers are partitioned into images or regions supporting different applications or activities. Therefore, while there may be one physical machine, it may be divided into four images, which is relevant to the scoping issue. Of these four images, two may be used to develop and test new applications or modifications to existing applications, and the other two images may be used for processing of significant computer applications. The latter two images, referred to as production images, are where the information systems auditor would want to concentrate control evaluation work. It would be important to determine and evaluate the environments provided by the operating system and security software that manage the processing and provides for its security. It is possible that different operating systems or versions and different security software are used for each production image. Such information is needed in planning for the staff skills needed to perform the control evaluation work.

VI.1.2 Determine whether general controls are likely to be effective

Page VI-2 shows that the next step, after obtaining background information, and identifying and obtaining an overview of each significant application, is to perform a preliminary assessment of the general controls (See section **2.3** of this manual).[1] This is accomplished primarily through inquiry and observation. This step can help avoid unnecessary control evaluation work, as significant control weaknesses may be identified with limited effort, such that the auditor assesses the general controls to be ineffective. **Appendix III** of this manual can help guide this assessment.

---

[1]Assessing inherent and control risks are important steps prior to this, but are not specifically depicted in the flow diagram on page VI-2. See section **2.2** of this manual for a discussion of this topic.

Appendix VI

However, if the general controls are determined to be likely ineffective, some control evaluation work is still advisable. Enough work should be done to identify over time significant weaknesses and their underlying causes that will lead to effective corrective actions. One of the purposes behind the legislation requiring the financial audits at federal agencies is to improve internal controls. Improvements will not result without the fundamental work that identifies control weaknesses and related corrective actions. Section **VI.3**, below, on rotation testing is an approach to planning work under these circumstances.

If the auditor determines that the general controls are likely to be effective, he/she should perform control tests to verify their effectiveness. Again, **Appendix III** can be used to guide this effort. For technical areas, such as access control software and operating systems, commercially available practice aids are helpful to guide evaluations.

VI.1.3 Determine whether application controls are likely to be effective

After performing the steps discussed above, if the auditor concludes that the general controls are effective, the effectiveness of the application controls needs to be determined. This step should not be done before determining the effectiveness of the general controls, as unnecessary control evaluation work may result. Ineffective general controls will render the application controls ineffective.

Not all application controls need to be evaluated. As mentioned previously, only applications that are significant to the financial statements warrant evaluation work. The concept of materiality, discussed in section **VI.2** can help determine which applications are significant to the financial statements. In addition, an extensive evaluation of controls within each significant application is not necessarily needed. As page VI-3 shows, the first action with application controls is to identify on the **Specific Control Evaluation (SCE) Form** those computer-related controls that will be used to reduce control risk and substantive testing. The controls listed on the **SCE** are the ones the auditor focuses on to determine their effectiveness. The responsibility to fill out the **SCE** rests primarily with the financial auditor, but the information systems auditor should be consulted in this process. The **SCE** generally contains both computer-related and non-computer-related controls.

VI.2 MATERIALITY

Materiality is a tool the auditor uses to determine that the planned nature, timing, and extent of audit procedures are appropriate. It is based on the concept that items of little importance, which do not affect the judgement or conduct of a reasonable user, do not require auditor investigation. Using this concept, the auditor may determine that some applications are not material, and therefore warrant little or no audit attention. Materiality is more fully discussed in the **Financial Audit Manual (FAM)** in section **230**.

VI.3 ROTATION TESTING OF CONTROLS

Rotation testing of controls can help reduce audit requirements under certain conditions. When appropriate, this concept allows the auditor to test computer-related application and general controls on a rotating basis rather than every year. Under a rotation plan, controls are tested in different applications or general control categories each year such that each significant application and general control category is selected for testing at least once during the rotation period, generally within 3 years. For example, a rotation plan for an entity with 5 significant applications might include tests of 2 or 3 applications annually, covering all applications in a 2 or 3 year period.

Rotation testing is not appropriate in all situations. For example, rotation testing is not appropriate for first-time audits, for audits where some significant applications or general control categories have not been tested within a sufficiently recent period of years, or for audits of entities that do not have a strong control environment. Also, this concept still requires that some limited tests be performed annually for applications and general control categories not selected for testing, such as updating the auditor's understanding of the control environment and conducting walk-throughs. For example, because of their importance, the auditor's understanding of the operating system and security software environments should be updated yearly. Rotation testing is discussed in greater detail in the **FAM** in section **395 G - Rotation Testing of Controls**.

VI.4 MULTIPLE-LOCATION AUDITS

Most federal entities conduct operations, perform accounting functions and/or retain records at multiple locations. Many entities have significant computer operations at regional or multi-located service centers. During planning, the auditor needs to consider the effect of these multiple locations on the audit approach. Performing an extensive level of audit activity at each location may not be necessary.

The auditor should develop an understanding of the respective locations, including significant accounts and accounting systems and applications associated with each

location. When planning locations to visit, the auditor should consider certain factors. For example, (1) locations more material to the entity and having significant applications may require more extensive testing; (2) locations at which inherent and/or control risks are high warrant more extensive testing than locations where they are low, which may be affected by the nature of the location's hardware and software used and the extent of resources potentially accessed from the location; and (3) a high degree of centralization may enable the auditor to conduct the majority of work at the central location, with only limited work at other locations, such as with centralized system development and modification activities when reviewing system change controls. This topic is further discussed in the **FAM**, in sections **285 - Plan Locations to Visit**, and **295 C - An Approach for Multiple-Location Audits**.

VI.5 CONTRACTING FOR AUDIT SERVICES

Contracting for audit services offers two significant benefits to an entity's audit organization–it allows audit coverage beyond that possible with the existing audit staff level, and it allows the audit activity to address technical and other issues in which the inhouse staff is not skilled. Such engagements may help train staff for future audits. However, contracting for audit services requires the active involvement of some inhouse audit personnel. For example, the audit organization should be instrumental in determining the scope of the contracted services, and in developing the task order for the work. Also, an auditor should be designated to monitor the contract for the entity. In this capacity, the contract monitor should conduct a meeting with the contractor to discuss the requirements of the contract. Discussions should include the product deliverables, the established time frames for deliverables, and work paper requirements, such as standards to adhere to. This meeting should be held prior to the time the contractor begins work. In addition, the contract monitor should attend all critical meetings the contractor has with entity representatives, including the opening and close-out briefings.

The contract monitor should conduct a technical review of the work performed and could use this manual as guidance to determine whether the work addressed relevant issues and the audit procedures were adequate. Some reperformance of testing should be done in accordance with **FAM 650**, "Using the Reports and Work of Others." Also, the contract monitor should review the audit report and supporting work papers to determine whether the audit report is supportable.

[This page intentionally left blank.]

Appendix VII

GLOSSARY

The definitions in this glossary are drawn from several sources, including this manual, certain IBM manuals, and the documents and sources listed in the bibliography. In addition, certain definitions were developed by project staff and independent public accounting firms.

Abend	(short for abnormal ending) An unexpected processing termination that may indicate that coding was incorrectly performed and that earlier testing was not adequate or not adequately controlled.
Acceptance testing	Final testing by users to decide whether they accept a new system.
Access control facility (CA-ACF2)	An access control software package marketed by Computer Associates International, Inc. (CA).
Access control software	(CA-ACF2, RACF, CA-TOP SECRET) This type of software, which is external to the operating system, provides a means of specifying who has access to a system, who has access to specific resources, and what capabilities authorized users are granted. Access control software can generally be implemented in different modes that provide varying degrees of protection such as denying access for which the user is not expressly authorized, allowing access which is not expressly authorized but providing a warning, or allowing access to all resources without warning regardless of authority.
Access control	Controls designed to protect computer resources from unauthorized modification, loss, or disclosure. Access controls include both physical access controls, which limit access to facilities and associated hardware, and logical controls, which prevent or detect unauthorized access to sensitive data and programs that are stored or transmitted electronically.
Access method	The technique used for selecting records in a file for processing, retrieval, or storage.
Access path	Sequence of hardware and software components significant to access control. Any component capable of enforcing access restrictions or any component that could be used to bypass an access restriction should be considered part of the access path. The access path can also be defined as the path through which user requests travel, including the telecommunications software, transaction processing software, application program, etc.
Access privileges	Precise statements that define the extent to which an individual can access computer systems and use or modify the programs and data on the system, and under what circumstances this access will be allowed.

Appendix VII

Accountability	The existence of a record that permits the identification of an individual who performed some specific activity so that responsibility for that activity can be established.
ACF2	See access control facility.
ADABAS	A relational database system developed by Software AG and implemented on mainframe and UNIX platforms. It uses relational attributes and also nonrelational techniques, such as multiple values and periodic groups. It has its own language called Natural.
American Standard Code for Information Interchange (ASCII)	A standard seven-bit code for representing 128-characters that was adopted by the American Standards Association to achieve compatibility between data devices.
APF	See authorized program facility.
Application	A computer program designed to help people perform a certain type of work, including specific functions, such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements.
Application controls	Application controls are directly related to individual applications. They help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.
Application programmer	A person who develops and maintains application programs, as opposed to system programmers who develop and maintain the operating system and system utilities.
Application programs	See application.
ASCII	See American standard code for information interchange.
Assembly language	A low-level procedural programming language in which each program statement corresponds directly to a single machine instruction. Assembly languages are thus specific to a given processor.

Assertion	Financial statement assertions are management representations that are embodied in financial statement components. The assertions can be either explicit or implicit and can be classified into the following broad categories: existence or occurrence (an entity's assets or liabilities exist at a given date and recorded transactions have occurred during a given period), completeness (all transactions and accounts that should be presented in the financial statements are so included), rights and obligations (assets are the rights of the entity, and liabilities are the obligations of the entity at a given date), valuation or allocation (asset, liability, revenue, and expense components have been included in the financial statements at appropriate amounts), and presentation and disclosure (the particular components of the financial statements are properly classified, described, and disclosed).
Audit risk	The risk that information or financial reports will contain material errors that the auditor may not detect.
Audit software	(ACL, IDEA) Generic audit software consists of a special program or set of programs designed to audit data stored on computer media. Audit software performs functions such as data extraction and reformatting, file creation, sorting, and downloading. This type of audit software may also be used to perform computations, data analysis, sample selection, summarization, file stratification, field comparison, file matching, or statistical analysis. (Panaudit, EDP Auditor, CA-EXAMINE) The term audit software may also refer to programs that audit specific functions, features, and controls associated with specific types of computer systems to evaluate integrity and identify security exposures.
Audit trail	In an accounting package, any program feature that automatically keeps a record of transactions so you can backtrack to find the origin of specific figures that appear on reports. In computer systems, a step-by-step history of a transaction, especially a transaction with security sensitivity. Includes source documents, electronic logs, and records of accesses to restricted files.
Authentication	The act of verifying the identity of a user and the user's eligibility to access computerized information. Designed to protect against fraudulent activity.
Authorized program facility	An operating system facility that controls which programs are allowed to use restricted system functions.

Backdoor	An undocumented way to gain access to a program, data, or an entire computer system, often known only to the programmer who created it. Backdoors can be handy when the standard way of getting information is unavailable, but they usually constitute a security risk.
Backup	Any duplicate of a primary resource function, such as a copy of a computer program or data file. This standby is used in case of loss or failure of the primary resource.
Backup procedures	A regular maintenance procedure that copies all new or altered files to a backup storage medium, such as a tape drive.
Bandwidth	The amount of data that can be transmitted via a given communications channel (such as a computer network) in a given unit of time (generally one second).
Batch processing	A mode of operation in which transactions are accumulated over a period of time, such as a day, week, or month, and then processed in a single run. In batch processing, users do not interact with the system while their programs and data are processing as they do during interactive processing.
Biometric authentication	The process of verifying or recognizing the identity of a person based on physiological or behavioral characteristics. Biometric devices include fingerprints, retina patterns, hand geometry, speech patterns, and keystroke dynamics.
BLP	See bypass label processing.
Bridge	A device that allows two networks, even ones dissimilar in topology, wiring, or communications protocols, to exchange data.
Browsing	The act of electronically perusing files and records without authorization.
Bug	A flaw in a computer program that causes it to produce incorrect or inappropriate results.
Bypass label processing (BLP)	A technique of reading a computer file while bypassing the internal file/data set label. This process could result in bypassing security access controls.
CA-ACF2	See access control facility.
CA-EXAMINE	An audit software package marketed by Computer Associates International, Inc. (CA) that can help identify and control MVS security exposures, viruses, Trojan horses, and logic bombs that can destroy production dependability and circumvent existing security mechanisms.
CA-TOP SECRET	See TOP SECRET.

Appendix VII

CAAT	See computer-assisted audit technique.
CD-ROM	See compact disk-read only memory.
Central processing unit (CPU)	The computational and control unit of a computer; the device that interprets and executes instructions.
Checkpoint	The process of saving the current state of a program and its data, including intermediate results to disk or other nonvolatile storage, so that if interrupted the program could be restarted at the point at which the last checkpoint occurred.
Chip	(also referred to as a microchip) Usually a silicon wafer on which circuit elements have been imprinted.
CICS	See customer information control system.
Cipher key lock	A lock with a key pad-like device that requires the manual entry of a predetermined code for entry.
Client/server model	A design model used on a network where individual workstations (clients) and shared servers work together to process applications. In this model, certain functions are allocated to the client workstations and the server. Typically, the server provides centralized, multiuser services, whereas the client workstations support user interaction.
CLIST	(short for command list) In TSO/E, CLISTS are programs that perform given tasks or groups of tasks. The most basic CLIST is a list of TSO/E commands. However, two command languages available in TSO/E (CLIST and REXX) provide the programming tools needed to create structured applications or manage programs written in other languages.
CobiT	See Control Objectives for Information and Related Technology.
COBOL	See common business-oriented language.
Code	Instructions written in a computer programming language. (See object code and source code.)
Cold site	An IS backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternative computing location.
Command	A job control statement or a message, sent to the computer system, that initiates a processing task.

Appendix VII

Common business-oriented language (COBOL)	A high-level programming language specially designed for business applications.
Communications program	A program that enables a computer to connect with another computer and exchange information by transmitting or receiving data over telecommunications networks.
Communications protocol	The standards that govern the transfer of information among computers on a network.
Compact disc-read only memory (CD-ROM)	Compact Disc (CD)-Read Only Memory (ROM) is a form of optical rather than magnetic storage. CD-ROM devices are generally read-only.
Compatibility	The capability of a computer, device, or program to function with or substitute for another make and model of computer, device, or program. Also, the capability of one computer to run the software written to run on another computer. Standard interfaces, languages, protocols, and data formats are key to achieving compatibility.
Compensating control	An internal control that reduces the risk of an existing or potential control weakness that could result in errors or omissions.
Compiler	A program that reads the statements in a human-readable programming language and translates them into a machine-readable executable program.
Component	A single resource with defined characteristics, such as a terminal or printer. These components are also defined by their relationship to other components.
Computer architecture	A general term referring to the structure of all or part of a computer system. The term also covers the design of system software, such as the operating system, as well as refers to the combination of hardware and basic software that links the machines on a computer network. Computer architecture refers to an entire structure and to the details needed to make it functional. Thus, computer architecture covers computer systems, circuits, and system programs, but typically does not cover applications, which are required to perform a task but not to make the system run.
Computer-assisted audit technique (CAAT)	Any automated audit technique, such as generalized audit software, test data generators, computerized audit programs, and special audit utilities.
Computer facility	A site or location with computer hardware where information processing is performed or where data from such sites are stored.

Computer operations	The function responsible for operating the computer and peripheral equipment, including providing the tape, disk, or paper resources as requested by the application systems.
Computer processing location	See computer facility.
Computer resource	See resource.
Computer room	Room within a facility that houses computers and/or telecommunication devices.
Computer system	A complete computer installation, including peripherals, in which all the components are designed to work with each other.
Computer-related controls	Computer-related controls help ensure the reliability, confidentiality, and availability of automated information. They include both general controls, which apply to all or a large segment of an entity's information systems, and application controls, which apply to individual applications.
Confidentiality	Ensuring that transmitted or stored data are not read by unauthorized persons.
Configuration management	The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system.
Console	Traditionally, a control unit such as a terminal through which a user communicates with a computer. In the mainframe environment, a console is the operator's station.
Contingency plan	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failure, or disaster.
Contingency planning	See contingency plan.
Control environment	The control environment is an important component of an entity's internal control structure. It sets the "tone at the top" and can influence the effectiveness of specific control techniques. Factors that influence the control environment include management's philosophy and operating style, the entity's organizational structure, methods of assigning authority and responsibility, management's control methods for monitoring and following up on performance, the effectiveness of the Inspector General and internal audit, personnel policies and practices, and influences external to the entity.

Appendix VII

Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and audit guidelines developed by the Information Systems Audit and Control Foundation (ISACF) as a generally applicable and accepted standard for good practices for controls over information technology.
Control risk	Risk that a material misstatement that could occur in an assertion will not be prevented, or detected and corrected on a timely basis by the entity's internal control structure.
Cooperative processing	A mode of operation in which two or more computers, such as a mainframe and a microcomputer, can carry out portions of the same program or work on the same data. It enables computers to share programs, workloads, and data files.
CPU	See central processing unit.
Cryptographic algorithm	A mathematical procedure used for such purposes as encrypting and decrypting messages and signing documents digitally.
Cryptographic system	The hardware, software, documents, and associated techniques and processes that together provide a means of encryption.
Cryptography	The science of coding messages so they cannot be read by any person other than the intended recipient. Ordinary text--or plain text--and other data are transformed into coded form by encryption and translated back to plain text or data by decryption.
Customer information control system (CICS)	An IBM communications system used for production applications in a mainframe environment. It facilitates the development of on-line applications and handles the concurrent processing of transactions entered from different terminals.
DASD	See direct access storage device.
Data	Facts and information that can be communicated and manipulated.
Data access method	See access method.
Data administration	The function that plans for and administers the data used throughout the entity. This function is concerned with identifying, cataloging, controlling, and coordinating the information needs of the entity.
Database	A collection of related information about a subject organized in a useful manner that provides a base or foundation for procedures, such as retrieving information, drawing conclusions, or making decisions. Any collection of information that serves these purposes qualifies as a database, even if the information is not stored on a computer.

Appendix VII

Database administrator (DBA)	The individual responsible for both the design of the database, including the structure and contents, and the access capabilities of application programs and users to the database. Additional responsibilities include operation, performance, integrity, and security of the database.
Database management	Tasks related to creating, maintaining, organizing, and retrieving information from a database.
Database management system (DBMS)	(DB2, IMS, IDMS) A software product that aids in controlling and using the data needed by application programs. DBMSs organize data in a database, manage all requests for database actions--such as queries or updates from users--and permit centralized control of security and data integrity.
Data center	See computer facility.
Data communications	The transfer of information from one computer to another through a communications medium, such as telephone lines, microwave relay, satellite link, or physical cable.
Data communications systems	See data communications.
Data control	The function responsible for seeing that all data necessary for processing is present and that all output is complete and distributed properly. This function is generally responsible for reconciling record counts and control totals submitted by users with similar counts and totals generated during processing.
Data definition	Identification of all fields in the database, how they are formatted, how they are combined into different types of records, and how the record types are interrelated.
Data dictionary	A repository of information about data, such as its meaning, relationships to other data, origin, usage, and format. The dictionary assists company management, database administrators, systems analysts, and application programmers in effectively planning, controlling, and evaluating the collection, storage, and use of data.
Data diddling	Changing data with malicious intent before or during input to the system.
Data encryption standard (DES)	A NIST Federal Information Processing Standard and a commonly used secret-key cryptographic algorithm for encrypting and decrypting data.
Data file	See file.
Data owner	See owner.

Data processing	The computerized preparation of documents and the flow of data contained in these documents through the major steps of recording, classifying, and summarizing.
Data processing center	See computer facility.
Data security	See security management function.
Data validation	Checking transaction data for any errors or omissions that can be detected by examining the data.
Data warehouse	A generic term for a system used to store, retrieve, and manage large amounts of data. A database, often remote, containing recent snapshots of corporate data that can be used for analysis without slowing down day-to-day operations of the production database.
DBA	See database administrator.
DBMS	See database management system.
Debug	With software, to detect, locate, and correct logical or syntactical errors in a computer program.
Decision support system (DSS)	An information system or analytic model designed to help managers and professionals be more effective in their decision-making.
Delete access	This level of access provides the ability to erase or remove data or programs.
DES	See data encryption standard.
Detection risk	The risk that the auditor will not detect a material misstatement that exists in an assertion.
Dial-up access	A means of connecting to another computer, or a network like the Internet, over a telecommunications line using a modem-equipped computer.
Dial-up security software	(Defender, Leehma) Software that controls access via remote dial-up. One method of preventing unauthorized users from accessing the system through an unapproved telephone line is through dial-back procedures in which the dial-up security software disconnects a call initiated from outside the network via dial-up lines, looks up the user's telephone number, and uses that number to call the user.
Direct access	An access method for finding an individual item on a storage device and accessing it directly, without having to access all preceding records.

Appendix VII

Direct access storage devices (DASD)	Any storage device, such as a hard disk, that provides the capability to access and/or manipulate data as required without having to access all preceding records to reach it. In contrast to direct or random access, sequential access devices, such as tape drives, require all preceding records to be read to reach the required data.
Disaster recovery plan	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
Disk storage	High-density random access magnetic storage devices that store billions of bits of data on round, flat plates that are either metal or plastic.
Diskette	A removable and widely used data storage medium that uses a magnetically coated flexible disk of Mylar enclosed in a plastic case.
Distributed processing	A mode of operation in which processing is spread among different computers that are linked through a communications network.
DSS	See decision support system.
Download	Process of transferring data from a central computer to a personal computer or workstation.
Dumb terminal	A terminal that serves only as an input/output mechanism linking a user with the central computer. This type of terminal does not have an internal processor.
Dump	To transfer the contents of memory to a printer or disk storage. Programmers use memory dumps to debug programs.
EBCDIC	See extended binary-coded decimal interchange code.
EDI	See electronic data interchange.
Electronic data interchange (EDI)	A standard for the electronic exchange of business documents, such as invoices and purchase orders. Electronic data interchange (EDI) eliminates intermediate steps in processes that rely on the transmission of paper-based instructions and documents by performing them electronically, computer to computer.
Electronic signature	A symbol, generated through electronic means, that can be used to (1) identify the sender of information and (2) ensure the integrity of the critical information received from the sender. An electronic signature may represent either an individual or an entity. Adequate electronic signatures are (1) unique to the signer, (2) under the signer's sole control, (3) capable of being verified, and (4) linked to the data in such a manner that if data are changed, the signature is invalidated upon verification. Traditional user identification code/password techniques do not meet these criteria.

Encryption	The transformation of data into a form readable only by using the appropriate key, held only by authorized parties.
End user computing	Any development, programming, or other activity where end users create or maintain their own systems or applications.
Environmental controls	This subset of physical access controls prevents or mitigates damage to facilities and interruptions in service. Smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies are some examples of environmental controls.
Execute access	This level of access provides the ability to execute a program.
Exit	A predefined or in-house written routine that receives controls at a predefined point in processing. These routines provide an entity with flexibility to customize processing, but also create the opportunity to bypass security controls.
Extended Binary-Coded Decimal Interchange Code (EBCDIC)	An eight-bit code developed by IBM for representing 256 characters.
Field	A location in a record in which a particular type of data are stored. In a database, the smallest unit of data that can be named. A string of fields is a concatenated field or record.
File	A collection of records stored in computerized form.
Financial information system	An information system that is used for one of the following functions: (1) collecting, processing, maintaining, transmitting, and reporting data about financial events, (2) supporting financial planning or budgeting activity, (3) accumulating and reporting cost information, or (4) supporting the preparation of financial statements.
Financial management system	Financial information systems and the financial portions of mixed systems (systems that support both financial and nonfinancial functions) that are necessary to support financial management.
Firewall	Firewalls are hardware and software components that protect one set of system resources (e.g., computers, networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users.
Floppy disk	A removable and widely used data storage medium that uses a magnetically coated flexible disk of Mylar enclosed in a plastic envelope.

Appendix VII

Flowchart	A diagram of the movement of transactions, computer functions, media, and/or operations within a system. The processing flow is represented by arrows between symbolic shapes for operation, device, data file, etc. to depict the system or program.
Flowcharter	Software that allows the user to prepare flowcharts. (See flowchart.)
Gateway	In networks, a computer that connects two dissimilar local area networks, or connects a local area network to a wide area network, minicomputer, or mainframe. A gateway may perform network protocol conversion and bandwidth conversion.
General controls	General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. They include an entitywide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls.
General support system	An interconnected set of information resources under the same direct management control that shares common functionality. Normally, the purpose of a general support system is to provide processing or communication support.
Hacker	A person who attempts to enter a system without authorization from a remote location.
Hardware	The physical components of information technology, including the computers, peripheral devices such as printers, disks, and scanners, and cables, switches, and other elements of the telecommunications infrastructure.
High level programming language	A programming language that provides a certain level of abstraction from the underlying machine language through the use of declarations, control statements, and other syntactical structures. In practice, the term refers to a computer language above assembly language.
Host computer	The main computer in a system of computers and terminals connected by communication links.
Hot site	A fully operational off-site data processing facility equipped with both hardware and system software to be used in the event of a disaster.
I/O appendage	See input/output appendage.
IDMS	A Cullinet Database Systems, Inc. database management system.
Implementation	The process of making a system operational in the organization.
IMS	See information management system.

Information	The meaning of data. Data are facts; they become information when they are seen in context and convey meaning to people.
Information Management System (IMS)	A general purpose IBM system product that allows users to access a database through remote terminals.
Information resource	See resource.
Information resource management	See information systems management.
Information resource owner	See owner.
Information systems management	The function that directs or manages the activities and staff of the IS department and its various organizational components.
Inherent risk	The susceptibility of an assertion to a material misstatement, assuming that there are no related internal controls.
Initial program load (IPL)	A program that brings another program, often the operating system, into operation to run the computer. Also referred to as a bootstrap or boot program.
Input	Any information entered into a computer or the process of entering data into the computer.
Input/output appendage	A routine designed to provide additional controls for system input/output operations.
Integration testing	Testing to determine if related information system components perform to specification.
Integrity	With respect to data, its accuracy, quality, validity, and safety from unauthorized use. This involves ensuring that transmitted or stored data are not altered by unauthorized persons in a way that is not detectable by authorized users.
Interactive processing	A mode of operation in which users interact with the system as their programs and data are processed.
Interface	A connection between two devices, applications, or networks or a boundary across which two systems communicate. Interface may also refer to the portion of a program that interacts with the user.

Appendix VII

Internal control	(also referred to as internal control structure) A process, effected by agency management and other personnel, designed to provide reasonable assurance that (1) operations, including the use of agency resources, are effective and efficient; (2) financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use, are reliable; and (3) applicable laws and regulations are followed. Internal control also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition. Internal control consists of five interrelated components that form an integrated process that can react to changing circumstances and conditions within the agency. These components include the control environment, risk assessment, control activities, information and communication, and monitoring.
Internet	When capitalized, the term "Internet" refers to the collection of networks and gateways that use the Transmission Control Protocol/Internet Protocol suite of protocols.
IPL	See initial program load.
JES2	See job entry system.
JES3	See job entry system.
Job	A set of data that completely defines a unit of work for a computer. A job usually includes programs, linkages, files, and instructions to the operating system.
Job accounting software	Software that tracks the computer resources (e.g., processor time and storage) used for each job.
Job control language (JCL)	In mainframe computing, a programming language that enables programmers to specify batch processing instructions. The abbreviation JCL refers to the job control language used in IBM mainframes.
Job entry system	(JES2, JES3) Software that allows the submission of programs from terminals (usually through on-line program development systems such as TSO) to the mainframe computer.
Job scheduling system	(CA-7, Manager, Scheduler) Software that queues the jobs submitted to be run on the mainframe. It uses job classes and other information provided by the person submitting the job to determine when the job will be run.
Key	A long stream of seemingly random bits used with cryptographic algorithms. The keys must be known or guessed to forge a digital signature or decrypt an encrypted message.
LAN	See local area network.

Appendix VII

Legacy system	A computer system, consisting of older applications and hardware, that was developed to solve a specific business problem. Many legacy systems do not conform to current standards, but are still in use because they solve the problem well and replacing them would be too expensive.
Library	In computer terms, a library is a collection of similar files, such as data sets contained on tape and/or disks, stored together in a common area. Typical uses are to store a group of source programs or a group of load modules. In a library, each program is called a member. Libraries are also called partitioned data sets (PDS). Library can also be used to refer to the physical site where magnetic media, such as a magnetic tape, is stored. These sites are usually referred to as tape libraries.
Library control/ management	The function responsible for controlling program and data files that are either kept on-line or are on tapes and disks that are loaded onto the computer as needed.
Library copier	Software that can copy source code from a library into a program.
Library management software	Software that provides an automated means of inventorying software, ensuring that differing versions are not accidentally misidentified, and maintaining a record of software changes.
Loader	A utility that loads the executable code of a program into memory for execution.
Load library	A partitioned data set used for storing load modules for later retrieval.
Load module	The results of the link edit process. An executable unit of code loaded into memory by the loader.
Local area network (LAN)	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables a device to interact with any other on the network. Local area networks (LAN) commonly include microcomputers and shared (often expensive) resources such as laser printers and large hard disks. Most modern LANs can support a wide variety of computers and other devices. Separate LANs can be connected to form larger networks.
Log	With respect to computer systems, to record an event or transaction.
Log off	The process of terminating a connection with a computer system or peripheral device in an orderly way.
Log on	The process of establishing a connection with, or gaining access to, a computer system or peripheral device.

Appendix VII

Logging file	See log.
Logic bomb	In programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.
Logical access control	The use of computer hardware and software to prevent or detect unauthorized access. For example, users may be required to input user identification numbers (ID), passwords, or other identifiers that are linked to predetermined access privileges.
Logical security	See logical access control.
Machine code	The program instructions that are actually read and executed by the computer's processing circuitry.
Mainframe computer	A multiuser computer designed to meet the computing needs of a large organization. The term came to be used generally to refer to the large central computers developed in the late 1950s and 1960s to meet the accounting and information management needs of large organizations.
Maintenance	Altering programs after they have been in use for a while. Maintenance programming may be performed to add features, correct errors that were not discovered during testing, or update key variables (such as the inflation rate) that change over time.
Major application	OMB Circular A-130 defines a major application as an application that requires special attention due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information in the application.
Management controls	The organization, policies, and procedures used to provide reasonable assurance that (1) programs achieve their intended result, (2) resources are used consistent with the organization's mission, (3) programs and resources are protected from waste, fraud, and mismanagement, (4) laws and regulations are followed, and (5) reliable and timely information is obtained, maintained, reported, and used for decision-making.
Master console	In MVS environments, the master console provides the principal means of communicating with the system. Other multiple console support (MCS) consoles often serve specialized functions, but can have master authority to enter all MVS commands.
Master file	In a computer, the most currently accurate and authoritative permanent or semipermanent computerized record of information maintained over an extended period.

Appendix VII

Material weakness	A material weakness is a reportable condition in which the design or operation of the internal controls does not reduce to a relatively low level the risk that losses, noncompliance, or misstatements in amounts that would be material in relation to the principal statements or to a performance measure or aggregation of related performance measures may occur and not be detected within a timely period by employees in the normal course of their assigned duties.
Materiality	An auditing concept regarding the relative importance of an amount or item. An item is considered as not material when it is not significant enough to influence decisions or have an effect on the financial statements.
Merge access	This level of access provides the ability to combine data from two separate sources.
Microchip	See chip.
Microcomputer	Any computer with its arithmetic-logic unit and control unit contained in one integrated circuit, called a microprocessor.
Microprocessor	An integrated circuit device that contains the miniaturized circuitry to perform arithmetic, logic, and control operations (i.e. contains the entire CPU on a single chip).
Midrange computer	A medium-sized computer with capabilities that fall between those of personal computers and mainframe computers.
Migration	A change from an older hardware platform, operating system, or software version to a newer one.
Modem	Short for modulator-demodulator. A device that allows digital signals to be transmitted and received over analog telephone lines. This type of device makes it possible to link a digital computer to the analog telephone system. It also determines the speed at which information can be transmitted and received.
Multiple virtual storage (MVS)	An IBM mainframe operating system. It has been superseded by OS/390 for IBM 390 series mainframes.
MVS	See multiple virtual storage.
Naming conventions	Standards for naming computer resources, such as data files, program libraries, individual programs, and applications.

Appendix VII

Network	A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communications links. A network can be as small as a local area network consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area.
Network administration	The function responsible for maintaining secure and reliable network operations. This function serves as a liaison with user departments to resolve network needs and problems.
Network architecture	The underlying structure of a computer network, including hardware, functional layers, interfaces, and protocols (rules) used to establish communications and ensure the reliable transfer of information. Because a computer network is a mixture of hardware and software, network architectures are designed to provide both philosophical and physical standards for enabling computers and other devices to handle the complexities of establishing communications links and transferring information without conflict. Various network architectures exist, among them the internationally accepted seven-layer open systems interconnection model and International Business Machine (IBM) Systems Network Architecture. Both the open systems interconnection model and the Systems Network Architecture organize network functions in layers, each layer dedicated to a particular aspect of communication or transmission and each requiring protocols that define how functions are carried out. The ultimate objective of these and other network architectures is the creation of communications standards that will enable computers of many kinds to exchange information freely.
Network master control system	(Netmaster, CA-VMAN) Software that controls the network providing monitoring information for reliability, stability, and availability of the network and traffic control and errors. These may also involve the use of special hardware.
Networked system	See network.
Node	In a local area network, a connection point that can create, receive, or repeat a message. Nodes include repeaters, file servers, and shared peripherals. In common usage, however, the term node is synonymous with workstation.
Nonrepudiation	The ability to prevent senders from denying that they have sent messages and receivers from denying that they have received messages.

Appendix VII

Object code	The machine code generated by a source code language processor such as an assembler or compiler. A file of object code may be immediately executable or it may require linking with other object code files, e.g., libraries, to produce a complete executable program.
Off-the-shelf software	Software that is marketed as a commercial product, unlike custom programs that are privately developed for a specific client.
On-line	A processing term that categorizes operations that are activated and ready for use. If a resource is on-line, it is capable of communicating with or being controlled by a computer. For example, a printer is on-line when it can be used for printing. An application is classified as on-line when users interact with the system as their information is being processed as opposed to batch processing.
On-line coding facility	See on-line program development software.
On-line debugging facility	Software that permits on-line changes to program object code with no audit trail. This type of software can activate programs at selected start points.
On-line editors	See on-line program development software.
On-line program development software	(TSO, ROSCOE, VOLLIE, ICCF, ISPF) Software that permits programs to be coded and compiled in an interactive mode.
On-line transaction monitor	(IMS/DC, CICS) In the mainframe environment, software that provides on-line access to the mainframe.
On-line transaction processing	On-line transaction processing records transactions as they occur.
Operating system	The software that controls the execution of other computer programs, schedules tasks, allocates storage, handles the interface to peripheral hardware, and presents a default interface to the user when no application program is running.
Operational controls	These controls relate to managing the entity's business and include policies and procedures to carry out organizational objectives, such as planning, productivity, programmatic, quality, economy, efficiency, and effectiveness objectives. Management uses these controls to provide reasonable assurance that the entity (1) meets its goals, (2) maintains quality standards, and (3) does what management directs it to do.
Output	Data/information produced by computer processing, such as graphic display on a terminal or hard copy.

Appendix VII

Output Devices	Peripheral equipment, such as a printer or tape drive, that provides the results of processing in a form that can be used outside the system.
Owner	Manager or director with responsibility for a computer resource, such as a data file or application program.
Parameter	A value that is given to a variable. Parameters provide a means of customizing programs.
PARMLIB	(Short for SYS1.PARMLIB) The partitioned data set that contains many initialization parameters that are used by an MVS operating system during an initial program load and by other system software components such as SMF that are invoked by operator command.
Partitioned data set (PDS)	Independent groups of sequentially organized records, called members, in direct access storage. Each member has a name stored in a directory that is part of the data set and contains the location of the member's starting point. PDSs are generally used to store programs. As a result, many are often referred to as libraries.
Password	A confidential character string used to authenticate an identity or prevent unauthorized access.
PDS	See partitioned data set.
Performance monitor	(Omegamon, Resolve, Deltamon) Software that tracks and records the speed, reliability, and other service levels delivered by a computer system.
Peripheral	A hardware unit that is connected to and controlled by a computer, but external to the CPU. These devices provide input, output, or storage capabilities when used in conjunction with a computer.
Personnel controls	This type of control involves screening individuals prior to their authorization to access computer resources. Such screening should be commensurate with the risk and magnitude of the harm the individual could cause.
Personnel security	See personnel controls.
Physical access control	This type of control involves restricting physical access to computer resources and protecting these resources from intentional or unintentional loss or impairment.
Physical security	See physical access control.
Piggy-backing	A method of gaining unauthorized access to a restricted area by entering after an authorized person but before the door closes and the lock resets. Piggy-backing can also refer to the process of electronically attaching to an authorized telecommunications link to intercept transmissions.

Appendix VII

Platform	The foundation technology of a computer system. Typically, a specific combination of hardware and operating system.
Port	An interface between the CPU of the computer and a peripheral device that governs and synchronizes the flow of data between the CPU and the external device.
Privileges	Set of access rights permitted by the access control system.
Processing	The execution of program instructions by the computer's central processing unit.
PPT	See program properties table.
Production control and scheduling	The function responsible for monitoring the information into, through, and as it leaves the computer operations area and for determining the succession of programs to be run on the computer. Often, an automated scheduling package is utilized in this task.
Production data	The data that supports the agency's operational information processing activities. It is maintained in the production environment as opposed to the test environment.
Production environment	The system environment where the agency performs its operational information processing activities.
Production programs	Programs that are being used and executed to support authorized organizational operations. Such programs are distinguished from "test" programs which are being developed or modified, but have not yet been authorized for use by management.
Profile	A set of rules that describes the nature and extent of access to available resources for a user or a group of users with similar duties, such as accounts payable clerks. (See standard profile and user profile.)
Program	A set of related instructions that, when followed and executed by a computer, perform operations or tasks. Application programs, user programs, system programs, source programs, and object programs are all software programs.
Program library	See library.
Program properties table (PPT)	A facility provided by IBM to identify programs that require special properties when invoked in an MVS environment. Although special properties may be required for an application to run efficiently, certain special properties also have security implications because they may allow the programs to bypass security authorization checking.
Programmer	A person who designs, codes, tests, debugs, and documents computer programs.

Appendix VII

Programming library software	(Panvalet, Librarian, Endeavor) A system that allows control and maintenance of programs for tracking purposes. The systems usually provide security, check out controls for programs, and on-line directories for information on the programs.
Proprietary	Privately owned, based on trade secrets, privately developed technology, or specifications that the owner refuses to divulge, thus preventing others from duplicating a product or program unless an explicit license is purchased.
Protocol	In data communications and networking, a standard that specifies the format of data as well as the rules to be followed when performing specific functions, such as establishing a connection and exchanging data.
Prototyping	A system development technique in which a working model of a new computer system or program is created for testing and refinement.
Public access controls	A subset of access controls that apply when an agency application promotes or permits public access. These controls protect the integrity of the application and public confidence in the application and include segregating the information made directly available to the public from official agency records.
Public domain software	Software that has been distributed with an explicit notification from the program's author that the work has been released for unconditional use, including for-profit distribution or modification by any party under any circumstances.
Quality assurance	The function that reviews software project activities and tests software products throughout the software life-cycle to determine if (1) the software project is adhering to its established plans, standards, and procedures, and (2) the software meets the functional specifications defined by the user.
Query	The process of extracting data from a database and presenting it for use.
RACF	See resource access control facility.
Read access	This level of access provides the ability to look at and copy data or a software program.
Real-time system	A computer and/or a software system that reacts to events before they become obsolete. This type of system is generally interactive and updates files as transactions are processed.
Record	A unit of related data fields. The group of data fields that can be accessed by a program and contains the complete set of information on a particular item.

Appendix VII

Regression testing	Selective retesting to detect faults introduced during modification of a system.
Reliability	The capability of hardware or software to perform as the user expects and to do so consistently, without failures or erratic behavior.
Remote access	The process of communicating with a computer located in another place over a communications link.
Remote job entry (RJE)	With respect to computer systems with locations geographically separate from the main computer center, submitting batch processing jobs via a data communications link.
Report writer software	(Easytrieve, SAS) Software that allows access to data to produce customized reports.
Reportable condition	Reportable conditions include matters coming to the auditor's attention that, in the auditor's judgment, should be communicated because they represent significant deficiencies in the design or operation of internal controls, which could adversely affect the entity's ability to meet its internal control objectives.
Resource	Something that is needed to support computer operations, including hardware, software, data, telecommunications services, computer supplies such as paper stock and preprinted forms, and other resources such as people, office facilities, and noncomputerized records.
Resource access control facility (RACF)	An access control software package developed by IBM.
Resource owner	See owner.
Risk assessment	The identification and analysis of possible risks in meeting the agency's objectives that forms a basis for managing the risks identified and implementing deterrents.
Risk management	A management approach designed to reduce risks inherent to system development and operations.
RJE	See remote job entry.
Router	An intermediary device on a communications network that expedites message delivery. As part of a LAN, a router receives transmitted messages and forwards them to their destination over the most efficient available route.
Run	A popular, idiomatic expression for program execution.

Appendix VII

Run manual	A manual that provides application-specific operating instructions, such as instructions on job setup, console and error messages, job checkpoints, and restart and recovery steps after system failures.
SDLC methodology	See system development life cycle methodology.
Security	The protection of computer facilities, computer systems, and data stored on computer systems or transmitted via computer networks from loss, misuse, or unauthorized access. Computer security, as defined by Appendix III to OMB Circular A-130, involves the use of management, personnel, operational, and technical controls to ensure that systems and applications operate effectively and provide confidentiality, integrity, and availability.
Security administrator	Person who is responsible for managing the security program for computer facilities, computer systems, and/or data that are stored on computer systems or transmitted via computer networks.
Security management function	The function responsible for the development and administration of an entity's information security program. This includes assessing risks, implementing appropriate security policies and related controls, establishing a security awareness and education program for employees, and monitoring and evaluating policy and control effectiveness.
Security plan	A written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security (the security management function) as well as those who own, use, or rely on the entity's computer resources.
Security profile	See profile.
Security program	The security program is an entitywide program for security planning and management that forms the foundation of an entity's security control structure and reflects senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.
Security software	See access control software.
Sensitive information	Any information that, if lost, misused, or accessed or modified in an improper manner, could adversely affect the national interest, the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act.

Server	A computer running administrative software that controls access to all or part of the network and its resources, such as disk drives or printers. A computer acting as a server makes resources available to computers acting as workstations on the network.
Service continuity controls	This type of control involves ensuring that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.
Simultaneous peripheral operations on-line (SPOOL)	In the mainframe environment, a component of system software that controls the transfer of data between computer storage areas with different speed capabilities. Usually, an intermediate device, such as a buffer, exists between the transfer source and the destination (e.g., a printer).
Smart card	A credit card sized token that contains a microprocessor and memory circuits for authenticating a user of computer, banking, or transportation services.
SMF	See system management facility.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Social engineering	A method used by hackers to obtain passwords for unauthorized access. Typically, this involves calling an authorized user of a computer system and posing as a network administrator.
Software	A computer program or programs, in contrast to the physical environment on which programs run (hardware).
Software life cycle	The phases in the life of a software product, beginning with its conception and ending with its retirement. These stages generally include requirements analysis, design, construction, testing (validation), installation, operation, maintenance, and retirement.
Source code	Human-readable program statements written in a high-level or assembly language, as opposed to object code, which is derived from source code and designed to be machine-readable.
SPOOL	See simultaneous peripheral operations on-line.
Spooling	A process of storing data to be printed in memory or in a file until the printer is ready to process it.
Stand-alone system	A system that does not require support from other devices or systems. Links with other computers, if any, are incidental to the system's chief purpose.

Appendix VII

Standard	In computing, a set of detailed technical guidelines used as a means of establishing uniformity in an area of hardware or software development.
Standard profile	A set of rules that describes the nature and extent of access to each resource that is available to a group of users with similar duties, such as accounts payable clerks.
Substantive testing	Substantive testing is performed to obtain evidence that provides reasonable assurance of whether the principal statements, and related assertions, are free of material misstatement. There are two general types of substantive tests: (1) substantive analytical procedures and (2) tests of details.
Supervisor call (SVC)	A supervisor call instruction interrupts a program being executed and passes control to the supervisor so that it can perform a specific service indicated by the instruction.
SVC	See supervisor call.
System administrator	The person responsible for administering use of a mulituser computer system, communications system, or both.
System analyst	A person who designs systems.
System designer	See system analyst.
System developer	See programmer.
System development life cycle (SDLC) methodology	The policies and procedures that govern software development and modification as a software product goes through each phase of its life cycle.
System life cycle	See software life cycle.
System management facility	An IBM control program that provides the means for gathering and recording information that can be used to evaluate the extent of computer system usage.
System programmer	A person who develops and maintains system software.
System software	The set of computer programs and related routines designed to operate and control the processing activities of computer equipment. It includes the operating system and utility programs and is distinguished from application software.
System startup	See initial program load.
System testing	Testing to determine that the results generated by the enterprise's information systems and their components are accurate and the systems perform to specification.
Tape library	The physical site where magnetic media is stored.

Appendix VII

Tape management system	(CA-1, TMS, EPAT) Software that controls and tracks tape files.
Technical controls	See logical access control.
Telecommunications	A general term for the electronic transmission of information of any type, such as data, television pictures, sound, or facsimiles, over any medium, such as telephone lines, microwave relay, satellite link, or physical cable.
Teleprocessing monitor	In the mainframe environment, a component of the operating system that provides support for on-line terminal access to application programs. This type of software can be used to restrict access to on-line applications and may provide an interface to security software to restrict access to certain functions within the application.
Terminal	A device consisting of a video adapter, a monitor, and a keyboard.
Test facility	A processing environment isolated from the production environment that is dedicated to testing and validating systems and/or their components.
Time-sharing	A technique that allows more than one individual to use a computer at the same time.
Time sharing option (TSO)	The time sharing option of MVS allows users to interactively share computer time and resources and also makes it easier for users to interact with MVS.
Token	In authentication systems, some type of physical device (such as a card with a magnetic strip or a smart card) that must be in the individual's possession in order to gain access. The token itself is not sufficient; the user must also be able to supply something memorized, such as a personal identification number (PIN).
TOP SECRET	An access control software package marketed by Computer Associates International, Inc. (CA).
Transaction	A discrete activity captured by a computer system, such as an entry of a customer order or an update of an inventory item. In financial systems, a transaction generally represents a business event that can be measured in money and entered in accounting records.
Transaction file	A group of one or more computerized records containing current business activity and processed with an associated master file. Transaction files are sometimes accumulated during the day and processed in batch production overnight or during off-peak processing periods.

Appendix VII

Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
TSO	See time-sharing option.
Unit testing	Testing individual program modules to determine if they perform to specification.
UNIX	A multitasking operating system originally designed for scientific purposes which has subsequently become a standard for midrange computer systems with the traditional terminal/host architecture. UNIX is also a major server operating system in the client/server environment.
Update access	This access level includes the ability to change data or a software program.
Upload	The process of transferring a copy of a file from a local computer to a remote computer by means of a modem or network.
User	The person who uses a computer system and its application programs to perform tasks and produce results.
User identification (ID)	A unique identifier assigned to each authorized computer user.
User profile	A set of rules that describes the nature and extent of access to each resource that is available to each user.
Utility program	Generally considered to be system software designed to perform a particular function (e.g., an editor or debugger) or system maintenance (e.g., file backup and recovery).
Validation	The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.
Virus	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate.
Wide area network (WAN)	A group of computers and other devices dispersed over a wide geographical area that are connected by communications links.
WAN	See wide area network.
Workstation	A microcomputer or terminal connected to a network. Workstation can also refer to a powerful, stand-alone computer with considerable calculating or graphics capability.

Appendix VII

Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
ZAP	A generic term used to define a type of program that can alter data and programs directly, bypassing controls. Because of this ability, the ZAP and SuperZAP programs must be secured from casual or unauthorized use.

Appendix VII

BIBLIOGRAPHY

Gartner Group. IT Glossary. Stamford, CT: Gartner Group, Inc., 1998. ***http://gartner12.gartnerweb.com/gg/static/itjournal/itglossary/gloscov.html*** (cited June 22, 1998).

Howe, Denis. The Free On-line Dictionary of Computing. United Kingdom: Denis Howe, 1998. ***http://wombat.doc.ic.ac.uk/*** (cited June 22, 1998).

McAtee, Bryan, ed. CISA Review Manual. Rolling Meadows, IL: Information Systems Audit and Control Association, 1995.

MDA Computing. Glossary. Croydon, Surrey, England: MDA Computing, Ltd., 1996. ***http://www.mdagroup.com/computing/homepage.htm*** (cited June 22, 1998).

Office of Management and Budget Circular A-123, Management Accountability and Control.

Office of Management and Budget Circular A-127, Financial Management Systems.

Office of Management and Budget Circular A-130, Revised February 8, 1996, (Transmittal Memorandum No. 3), Appendix III, Security of Federal Automated Information Resources.

Paulk, M.C., C.V. Weber, S.M. Garcia, M.B. Chrissis, and M. Bush. Key Practices of the Capability Maturity Model (SM). Pittsburgh, PA: Carnegie Mellon University, 1993.

Pfaffenberger, Bryan. Webster's New World Dictionary of Computer Terms, 6th ed. New York, NY: Simon & Schuster, Inc., 1997.

Schlaikjer, Marjorie, ed. Computer Dictionary: The Comprehensive Standard for Business, School, Library, and Home. Redmond, WA: Microsoft Press, 1991.

U.S. General Accounting Office. Financial Audit Manual. GAO/AIMD-12.19.5A.

U.S. General Accounting Office. Year 2000 Computing Crisis: An Assessment Guide. GAO/AIMD-10.1.14, September 1997.

U.S. General Accounting Office. Information Superhighway: An Overview of Technology Challenges. GAO/AIMD-95-23, January 1995.

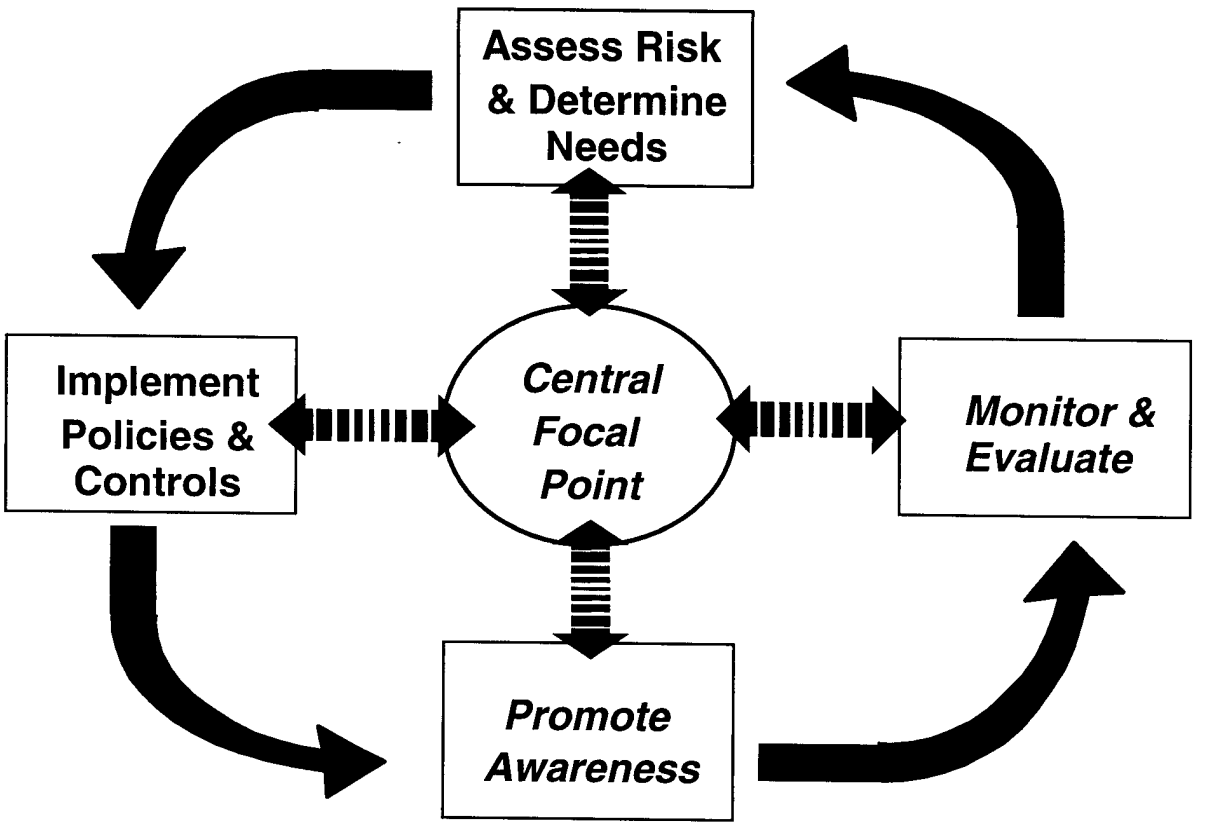
Warren, J.D., Jr., L.W. Edelson, and X.L. Parker. Handbook of IT Auditing. Boston, MA: Warren, Gorham & Lamont, 1996.

[This page intentionally left blank.]

Appendix VIII

PRINCIPLES FOR MANAGING AN INFORMATION SECURITY PROGRAM

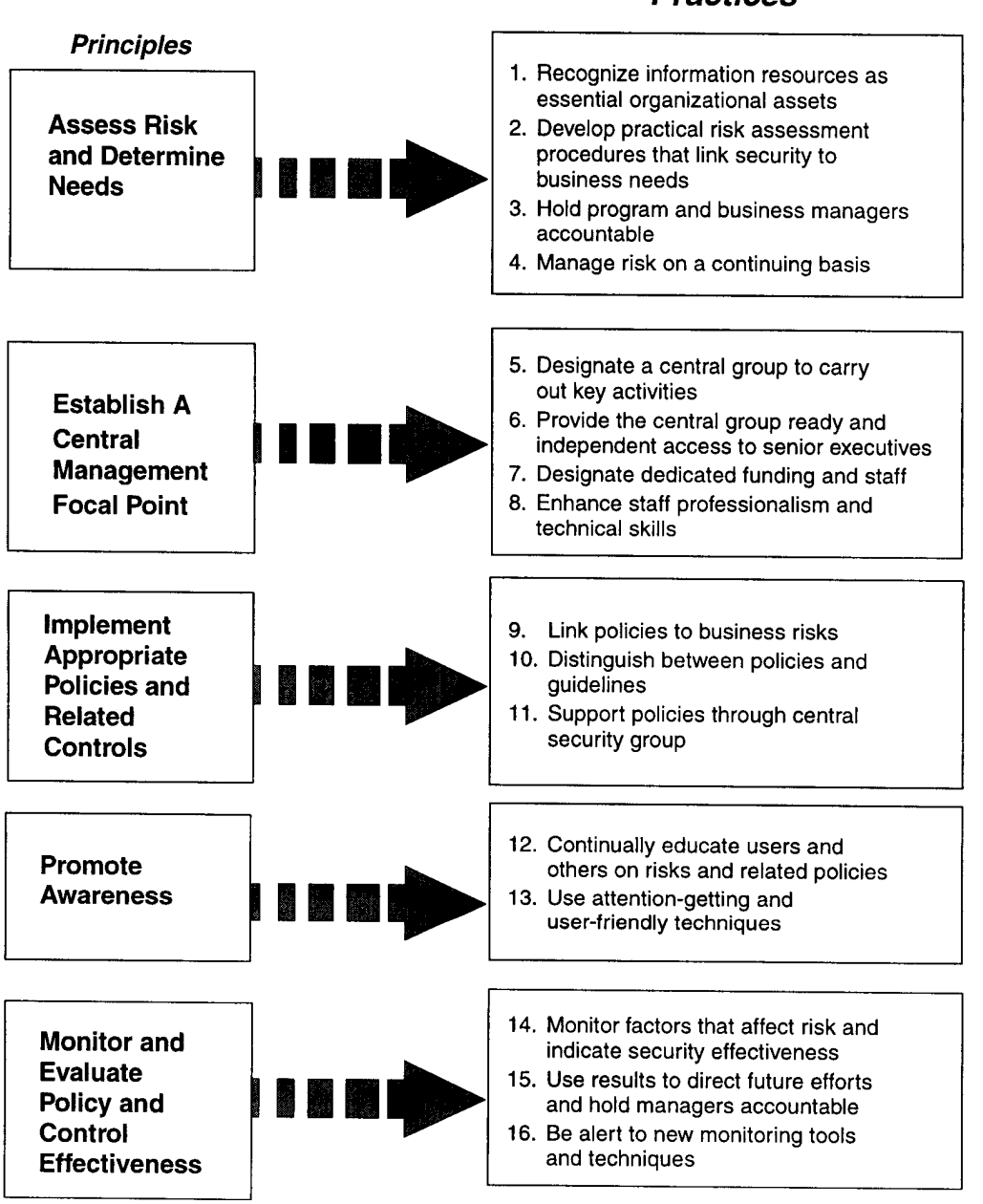
Risk Management Cycle[1]



[1]Source: Executive Guide: Information Security Management, Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).

Appendix VIII

Sixteen Practices Employed by Leading Organizations To Implement the Risk Management Cycle[2]



[2]Source: Executive Guide: Information Security Management, Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).

Appendix VIII

Security Objective, Core Principles, and Approach for Managing Information Security[3]

Security Objective: The objective of information security is the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity.

Core Principles

Accountability: Responsibility and accountability must be explicit.

Awareness: Awareness of risks and security initiatives must be disseminated.

Multidisciplinary: Security must be addressed taking into consideration both technological and non-technological issues.

Proportionality: Security must be cost-effective.

Integration: Security must be coordinated and integrated.

Reassessment: Security must be reassessed periodically.

Timeliness: Security procedures must provide for monitoring and timely response.

Societal Factors: Ethics must be promoted by respecting the rights and interests of others.

Approach

Policy Development: The security objective and core principles provide a framework for the first critical step for any organization - developing a security policy.

Roles and Responsibilities: For security to be effective, it is imperative that individual roles, responsibilities, and authority are clearly communicated and understood by all.

---

[3]International Federation of Accountants, Managing Security of Information and Communications, June 1997

Appendix VIII

Design: Once a policy has been approved by the governing body of the organization and related roles and responsibilities assigned, it is necessary to develop a security and control framework that consists of standards, measures, practices, and procedures.

Implementation: Once the design of the security standards, measures, practices, and procedures has been approved, the solution should be implemented on a timely basis, and then maintained.

Monitoring: Monitoring measures need to be established to detect and ensure correction of security breaches, such that all actual and suspected breaches are promptly identified, investigated, and acted upon, and to ensure ongoing compliance with policy, standards, and minimum acceptable security practices.

Awareness, Training, and Education: Awareness of the need to protect information, training in the skills needed to operate them securely, and education in security measures and practices are of critical importance for the success of an organization's security program.

MAJOR CONTRIBUTORS TO THIS AUDIT MANUAL

Accounting and Information Management Division, Washington, DC	Robert F. Dacey, Director-Consolidated Audit and Computer Security Issues Darrell L. Heim, Assistant Director-in-Charge Abraham D. Akresh, Assistant Director Jean L. Boltz, Assistant Director Carol A. Langelier, Assistant Director Crawford L. (Les) Thompson, Assistant Director Gary R. Austin, Senior Information Systems Analyst Janet Eackloff, Reports Analyst
Atlanta Field Office	Sharon S. Kittrell, Senior EDP Auditor
Dallas Field Office	David W. Irvin, Assistant Director Shannon Q. Cross, Senior EDP Auditor William H. Thompson, Senior EDP Auditor Charles M. Vrabel, Senior EDP Auditor Debra M. Conner, Senior EDP Auditor

[This page intentionally left blank.]

Appendix X

SUBMITTING COMMENTS ON FISCAM

Comments on this manual are encouraged. The following form is provided to assist in making comments. This form, and other written comments, should be sent to the following address:

U.S. General Accounting Office
Accounting and Information Management Division
Room 5T37
441 G St., NW
Washington, D.C. 20548

Attn: Robert F. Dacey, Director - CACSI

Comments may also be sent by e-mail to the following:

heimd.aimd@gao.gov

FISCAM Comments			
Name/Title:	Phone:		
Organization/Mailing Address:	E-mail:		
	Date:		
	Would you like a reply? (check one)		Yes
			No
Applicable FISCAM Section:			
Accuracy:			
Completeness:			
Organization:			
Clarity:			
Other: Please do not write below this line.			
Action:	Date:		

FISCAM Comments			
Name/Title:	Phone:		
Organization/Mailing Address:	E-mail:		
	Date:		
	Would you like a reply? (check one)		Yes
			No
Applicable FISCAM Section:			
Accuracy:			
Completeness:			
Organization:			
Clarity:			
Other: Please do not write below this line.			
Action:	Date:		

FISCAM Comments			
Name/Title:	Phone:		
Organization/Mailing Address:	E-mail:		
	Date:		
	Would you like a reply? (check one)		Yes
			No
Applicable FISCAM Section:			
Accuracy:			
Completeness:			
Organization:			
Clarity:			
Other: Please do not write below this line.			
Action:	Date:		