CIO COUNCIL

Federal Chief Information Officers Council

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: CHIEF INFORMATION OFFICERS COUNCIL
SALLY KATZEN, CHAIR & Deputy Director for Management, OMB
JAMES FLYZIK, VICE CHAIR & CIO, TREASURY

SUBJECT: Federal Information Technology Security Assessment Framework

The Chief Information Officers (CIO) Council's Federal Information Technology (IT) Security Assessment Framework provides a method for agency officials to determine the current status of their security programs relative to existing requirements and, where necessary, to establish a target for improvement. Consistent with Office of Management and Budget (OMB) policy, agencies must implement and maintain programs to adequately secure their information and system assets. This Framework was developed in cooperation by the CIO Council's Security, Privacy, and Critical Infrastructure Committee with OMB, and the National Institute of Standards and Technology (NIST). It is based upon requirements found in OMB's security policies, the General Accounting Office's Federal Information System Controls Audit Manual, and NIST's recommended security practices.

The attached Framework comprises five levels to guide agency assessment of their security status and assist in prioritizing efforts for improvement. A companion to the Framework, a NIST prepared self-assessment questionnaire, will provide specific questions that identify the control criteria against which agencies can determine the security status of an asset, a program, and the entire agency. This questionnaire will be issued early next year.

The importance of assessing the effectiveness of programs and security controls is key to achieving and maintaining adequate security. In fact, the recently enacted Government Information Security Reform Act, part of the FY 2001 Defense Authorization Act (P.L. 106-398), requires annual agency program reviews and Inspector General audits of information security programs and practices. Together with upcoming guidance on implementing the new Act, the Framework and forthcoming questionnaire will assist agencies in performing these reviews.

We recommend agencies allow sufficient time, at least six months, to perform assessments in light of these new reporting requirements. Questions on the Framework or the upcoming NIST questionnaire should be directed to Marianne Swanson, (301) 975-3293, marianne.swanson@nist.gov.

Sally Katzen
Sally Katzen
Chair, CIO Council

Jim Flyzik
Jim Flyzik
Vice Chair, CIO Council

Attachment

GAO

Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

December 4, 2000

The Honorable Sally Katzen
Chair, Chief Information Officers Council

Dear Ms. Katzen:

We commend the federal Chief Information Officers Council for encouraging agencies to routinely evaluate the status of their information security programs and for providing this Security Assessment Framework as a tool for facilitating such efforts. We appreciate having had an opportunity to participate in its initial development.

Ongoing self-assessments are an essential element of good management. Only by measuring progress and evaluating the effectiveness of policies and controls can management determine where improvements are needed. This is especially true for information security programs, where the effectiveness of efforts to reduce the risks of tampering, disruption, and inappropriate disclosure may not be immediately apparent.

This Security Assessment Framework is intended to be the foundation for a more detailed and complete set of tools that will include a series of questionnaires on specific areas of control, such as those pertaining to access and service continuity. We believe that these questionnaires will provide important specific guidance and, thus, will be essential to the framework's success.

Until these questionnaires are available, we encourage agency managers to begin using the criteria already identified in the framework and to provide comments on its usefulness to the CIO Council. By supporting the Security Assessment Framework in this manner, agencies can help ensure that it becomes a valuable tool and a basis for consistently evaluating the status of information security from a governmentwide perspective.

Sincerely yours,

Joel Willemssen
Managing Director, Information Technology Issues

Federal Information Technology Security Assessment Framework

November 28, 2000

Prepared for

Security, Privacy, and Critical Infrastructure Committee

by

National Institute of Standards and Technology (NIST)
Computer Security Division
Systems and Network Security Group

Overview

Information and the systems that process it are among the most valuable assets of any organization. Adequate security of these assets is a fundamental management responsibility. Consistent with Office of Management and Budget (OMB) policy, each agency must implement and maintain a program to adequately secure its information and system assets. Agency programs must: 1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability; and 2) protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

Agencies must plan for security, and ensure that the appropriate officials are assigned security responsibility and authorize system processing prior to operations and periodically thereafter. These management responsibilities presume that responsible agency officials understand the risks and other factors that could negatively impact their mission goals. Moreover, these officials must understand the current status of security programs and controls in order to make informed judgements and investments that appropriately mitigate risks to an acceptable level.

The Federal Information Technology (IT) Security Assessment Framework (or Framework) provides a method for agency officials to 1) determine the current status of their security programs relative to existing policy and 2) where necessary, establish a target for improvement. It does not establish new security requirements. The Framework may be used to assess the status of security controls for a given asset or collection of assets. These assets include information, individual systems (e.g., major applications, general support systems, mission critical systems), or a logically related grouping of systems that support operational programs, or the operational programs themselves (e.g., Air Traffic Control, Medicare, Student Aid). Assessing all asset security controls and all interconnected systems that the asset depends on produces a picture of both the security condition of an agency component and of the entire agency.

The Framework comprises five levels to guide agency assessment of their security programs and assist in prioritizing efforts for improvement. Coupled with the NIST-prepared self-assessment questionnaire[1], the Framework provides a vehicle for consistent and effective measurement of the security status for a given asset. The security status is measured by determining if specific security controls are documented, implemented, tested and reviewed, and incorporated into a cyclical review/improvement program, as well as whether unacceptable risks are identified and mitigated. The NIST questionnaire provides specific questions that identify the control criteria against which agency policies, procedures, and security controls can be compared. Appendix A contains a sample of the upcoming NIST Special Publication.

The Framework is divided into five levels: Level 1 of the Framework reflects that an asset has documented security policy. At level 2, the asset also has documented procedures and controls to implement the policy. Level 3 indicates that procedures and

[1] The NIST Self-assessment Questionnaire will be issued in 2001 as a NIST Special Publication.

controls have been implemented. Level 4 shows that the procedures and controls are tested and reviewed. At level 5, the asset has procedures and controls fully integrated into a comprehensive program. Each level represents a more complete and effective security program. OMB and the Council recognize that the security needs for the tens of thousands of Federal information systems differ. Agencies should note that testing the effectiveness of the asset and all interconnected systems that the asset depends on is essential to understanding whether risk has been properly mitigated. When an individual system does not achieve level 4, agencies should determine whether that system meets the criteria found in OMB Memorandum M00-07 (February 28, 2000) “Incorporating and Funding Security in Information Systems Investments.” Agencies should seek to bring all assets to level 4 and ultimately level 5.

Integral to all security programs whether for an asset or an entire agency is a risk assessment process that includes determining the level of sensitivity of information and systems. Many agencies have developed their own methods of making these determinations. For example, the Department of Health and Human Services uses a four--track scale for confidentiality, integrity, and availability. The Department of Energy uses five groupings or “clusters” to address sensitivity. Regardless of the method used, the asset owner is responsible for determining how sensitive the asset is, what level of risk is acceptable, and which specific controls are necessary to provide adequate security to that asset. Again, each implemented security control must be periodically tested for effectiveness. The decision to implement and the results of the testing should be documented.

1. Framework Description

The Federal Information Technology Security Assessment Framework (Framework) identifies five levels of IT security program effectiveness (see Figure 1). The five levels measure specific management, operational, and technical control objectives. Each of the five levels contains criteria to determine if the level is adequately implemented. For example, in Level 1 all written policy should contain the purpose and scope of the policy, who is responsible for implementing the policy, and the consequences and penalties for not following the policy. The policy for an individual control must be reviewed to ascertain that the criteria for level 1 are met. Assessing the effectiveness of the individual controls, not simply their existence, is key to achieving and maintaining adequate security.

The asset owner, in partnership with those responsible for administering the information assets (which include IT systems), must determine whether the measurement criteria are being met at each level. Before making such a determination, the degree of sensitivity of information and systems must be determined by considering the requirements for confidentiality, integrity, and availability of both the information and systems -- the value of information and systems is one of the major factors in risk management.

A security program may be assessed at various levels within an organization. For example, a program could be defined as an agency asset, a major application, general support system, high impact program, physical plant, mission critical system, or logically related group of systems. The Framework refers to this grouping as an asset.

The Framework describes an asset self-assessment and provides levels to guide and prioritize agency efforts as well as a basis to measure progress. In addition, the National Institute of Standards and Technology (NIST) will develop a questionnaire that gives the implementation tools for the Framework. The questionnaire will contain specific control objectives that should be applied to secure a system.

Figure 1 – Federal IT Security Assessment Framework

Level 1	**Documented Policy**
Level 2	**Documented Procedures**
Level 3	**Implemented Procedures and Controls**
Level 4	**Tested and Reviewed Procedures and Controls**
Level 5	**Fully Integrated Procedures and Controls**

The Framework approach begins with the premise that all agency assets must meet the minimum security requirements of the Office of Management and Budget Circular A-130, “Management of Federal Resources”, Appendix III, “Security of Federal Automated Information Resources” (A-130). The criteria that are outlined in the Framework and provided in detail in the questionnaire are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy. It should be noted that an agency might have additional laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability. Each agency should decide if additional security controls should be added to the questionnaire and, if so, customize the questionnaire appropriately. A list of the documents that the Framework and the questionnaire draw upon are provided in Figure 2.

Figure 2 – Source of Control Criteria

Office of Management and Budget Circular A-130, "Management of Federal Information Resources", Appendix III, "Security of Federal Automated Information Resources."	Establishes a minimum set of controls to be included in Federal IT security programs.
Computer Security Act of 1987.	This statute set the stage for protecting systems by codifying the requirement for Government-wide IT security planning and training.
Paperwork Reduction Act of 1995.	The PRA established a comprehensive information resources management framework including security and subsumed the security responsibilities of the Computer Security Act of 1987.
Clinger-Cohen Act of 1996.	This Act linked security to agency capital planning and budget processes, established agency Chief Information Officers, and re-codified the Computer Security Act of 1987.
Presidential Decision Directive 63, "Protecting America's Critical Infrastructures."	This directive specifies agency responsibilities for protecting the nation's infrastructure; assessing vulnerabilities of public and private sectors; and eliminating vulnerabilities.
Presidential Decision Directive 67, "Enduring Constitutional Government and Continuity of Government."	Relates to ensuring constitutional government, continuity of operations (COOP) planning, and continuity of government (COG) operations
OMB Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records."	This memorandum provides instructions to agencies on how to comply with the President's Memorandum of May 14, 1998 on "Privacy and Personal Information in Federal Records."
OMB Memorandum 99-18, "Privacy Policies on Federal Web Sites."	This memorandum directs Departments and Agencies to post clear privacy policies on World Wide Web sites, and provides guidance for doing so.
OMB Memorandum 00-13, "Privacy Policies and Data Collection on Federal Web Sites."	The purpose of this memorandum is a reminder that each agency is required by law and policy to establish clear privacy policies for its web activities and to comply with those policies.
General Accounting Office "Federal Information System Control Audit Manual" (FISCAM).	The FISCAM methodology provides guidance to auditors in evaluating internal controls over the confidentiality, integrity, and availability of data maintained in computer-based information systems.
NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Security Information Technology Systems."	This publication guides organizations on the types of controls, objectives, and procedures that comprise an effective security program.
NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems."	This publication details the specific controls that should be documented in a security plan.
Federal Information Processing Standards.	This document contains legislative and executive mandates for improving the utilization and management of computers and IT systems in the Federal Government.

2. Documented Policy - Level 1

2.1 Description

Level 1 of the Framework includes:

- Formally documented and disseminated security policy covering agency headquarters and major components (e.g., bureaus and operating divisions). The policy may be asset specific.
- Policy that references most of the basic requirements and guidance issued from the documents listed in Figure 2 – Source of Control Criteria.

An asset is at level 1 if there is a formally, up-to-date documented policy that establishes a continuing cycle of assessing risk, implements effective security policies including training, and uses monitoring for program effectiveness. Such a policy may include major agency components, (e.g., bureaus and operating divisions) or specific assets.

A documented security policy is necessary to ensure adequate and cost effective organizational and system security controls. A sound policy delineates the security management structure and clearly assigns security responsibilities, and lays the foundation necessary to reliably measure progress and compliance. The criteria listed below should be applied when assessing the policy developed for the controls that are listed in the NIST questionnaire.

2.2 Criteria

Level 1 criteria describe the components of a security policy.

Criteria for Level 1
a. Purpose and scope. An up-to-date security policy is written that covers all major facilities and operations agency-wide or for the asset. The policy is approved by key affected parties and covers security planning, risk management, review of security controls, rules of behavior, life-cycle management, processing authorization, personnel, physical and environmental aspects, computer support and operations, contingency planning, documentation, training, incident response, access controls, and audit trails. The policy clearly identifies the purpose of the program and its scope within the organization.
b. Responsibilities. The security program comprises a security management structure with adequate authority, and expertise. IT security manager(s) are appointed at an overall level and at appropriate subordinate levels. Security responsibilities and expected behaviors are clearly defined for asset owners and users, information resources management and data processing personnel, senior management, and security administrators.
c. Compliance. General compliance and specified penalties and disciplinary actions are also identified in the policy.

3. Documented Procedures - Level 2

3.1 Description

Level 2 of the Framework includes:

- Formal, complete, well-documented procedures for implementing policies established at level one.
- The basic requirements and guidance issued from the documents listed in Figure 2 – Source of Control Criteria.

An asset is at level 2 when formally documented procedures are developed that focus on implementing specific security controls. Formal procedures promote the continuity of the security program. Formal procedures also provide the foundation for a clear, accurate, and complete understanding of the program implementation. An understanding of the risks and related results should guide the strength of the control and the corresponding procedures. The procedures document the implementation of and the rigor in which the control is applied. Level 2 requires procedures for a continuing cycle of assessing risk and vulnerabilities, implementing effective security policies, and monitoring effectiveness of the security controls. Approved system security plans are in place for all assets.

Well-documented and current security procedures are necessary to ensure that adequate and cost effective security controls are implemented. The criteria listed below should be applied when assessing the quality of the procedures for controls outlined in the NIST questionnaire.

3.2 Criteria

Level 2 criteria describe the components of security procedures.

Criteria for Level 2
a. Control areas listed and organization's position stated. Up-to-date procedures are written that covers all major facilities and operations within the asset. The procedures are approved by key responsible parties and cover security policies, security plans, risk management, review of security controls, rules of behavior, life-cycle management, processing authorization, personnel, physical and environmental aspects, computer support and operations, contingency planning, documentation, training, incident response, access controls, and audit trails. The procedures clearly identify management's position and whether there are further guidelines or exceptions.
b. Applicability of procedures documented. Procedures clarify where, how, when, to, whom, and about what a particular procedure applies.
c. Assignment of IT security responsibilities and expected behavior. Procedures clearly define security responsibilities and expected behaviors for (1) asset owners and users, (2) information resources management and data processing personnel, (3) management, and (4) security administrators.
d. Points of contact and supplementary information provided. Procedures contain appropriate individuals to be contacted for further information, guidance, and compliance.

4. Implemented Procedures and Controls - Level 3

4.1 Description

Level 3 of the Framework includes:

- Security procedures and controls that are implemented.
- Procedures that are communicated and individuals who are required to follow them.

At level 3, the IT security procedures and controls are implemented in a consistent manner and reinforced through training. Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged. Security controls for an asset could be implemented and not have procedures documented, but the addition of formal documented procedures at level 2 represents a significant step in the effectiveness of implementing procedures and controls at level 3. While testing the on-going effectiveness is not emphasized in level 3, some testing is needed when initially implementing controls to ensure they are operating as intended. The criteria listed below should be used to determine if the specific controls listed in the NIST questionnaire are being implemented.

4.2 Criteria

Level 3 criteria describe how an organization can ensure implementation of their security procedures.

Criteria for Level 3
a. Owners and users are made aware of security policies and procedures. Security policies and procedures are distributed to all affected personnel, including system/application rules and expected behaviors. Requires users to periodically acknowledge their awareness and acceptance of responsibility for security.
b. Policies and procedures are formally adopted and technical controls installed. Automated and other tools routinely monitor security. Established policy governs review of system logs, penetration testing, and internal/external audits.
c. Security is managed throughout the life cycle of the system. Security is considered in each of the life-cycle phases: initiation, development/acquisition, implementation, operation, and disposal.
d. Procedures established for authorizing processing (certification and accreditation). Management officials must formally authorize system operations and manage risk.
e. Documented security position descriptions. Skill needs and security responsibilities in job descriptions are accurately identified.
f. Employees trained on security procedures. An effective training and awareness program tailored for varying job functions is planned, implemented, maintained, and evaluated.

5. Tested and Evaluated Procedures and Controls - Level 4

5.1 Description

Level 4 of the Framework includes:

- Routinely evaluating the adequacy and effectiveness of security policies, procedures, and controls.

- Ensuring that effective corrective actions are taken to address identified weaknesses, including those identified as a result of potential or actual security incidents or through security alerts issued by FedCIRC, vendors, and other trusted sources.

Routine evaluations and response to identified vulnerabilities are important elements of risk management, which includes identifying, acknowledging, and responding, as appropriate, to changes in risk factors (e.g., computing environment, data sensitivity) and ensuring that security policies and procedures are appropriate and are operating as intended on an ongoing basis.

Routine self-assessments are an important means of identifying inappropriate or ineffective security procedures and controls, reminding employees of their security-related responsibilities, and demonstrating management's commitment to security. Self-assessments can be performed by agency staff or by contractors or others engaged by agency management. Independent audits such as those arranged by the General Accounting Office (GAO) or an agency Inspector General (IG), are an important check on agency performance, but should not be viewed as a substitute for evaluations initiated by agency management.

To be effective, routine evaluations must include tests and examinations of key controls. Reviews of documentation, walk-throughs of agency facilities, and interviews with agency personnel, while providing useful information, are not sufficient to ensure that controls, especially computer-based controls, are operating effectively. Examples of tests that should be conducted are network scans to identify known vulnerabilities, analyses of router and switch settings and firewall rules, reviews of other system software settings, and tests to see if unauthorized system access is possible (penetration testing). Tests performed should consider the risks of authorized users exceeding authorization as well as unauthorized users (e.g., external parties, hackers) gaining access. Similar to levels 1 through 3, to be meaningful, evaluations must include security controls of interconnected assets, e.g., network supporting applications being tested.

When assets are first implemented or are modified, they should be tested and certified to ensure that controls are initially operating as intended. (This would occur at Level 3.) Requirements for subsequent testing and recertification should be integrated into an agency's ongoing test and evaluation program.

In addition to test results, agency evaluations should consider information gleaned from records of potential and actual security incidents and from security alerts, such as those issued by software vendors. Such information can identify specific vulnerabilities and provide insights into the latest threats and resulting risks.

The criteria listed below should be applied to each control area listed in the NIST questionnaire to determine if the asset is being effectively evaluated.

5.2 Criteria

Level 4 criteria are listed below.

Criteria for Level 4
a. Effective program for evaluating adequacy and effectiveness of security policies, procedures, and controls. Evaluation requirements, including requirements regarding the type and frequency of testing, should be documented, approved, and effectively implemented. The frequency and rigor with which individual controls are tested should depend on the risks that will be posed if the controls are not operating effectively. At a minimum, controls should be evaluated whenever significant system changes are made or when other risk factors, such as the sensitivity of data processed, change. Even controls for inherently low-risk operations should be tested at a minimum of every 3 years.
b. Mechanisms for identifying vulnerabilities revealed by security incidents or security alerts. Agencies should routinely analyze security incident records, including any records of anomalous or suspicious activity that may reveal security vulnerabilities. In addition, they should review security alerts issued by FedCIRC, vendors, and others.
c. Process for reporting significant security weaknesses and ensuring effective remedial action. Such a process should provide for routine reports to senior management on weaknesses identified through testing or other means, development of action plans, allocation of needed resources, and follow-up reviews to ensure that remedial actions have been effective. Expedited processes should be implemented for especially significant weaknesses that may present undue risk if not addressed immediately.

6. Fully Integrated Procedures and Controls - Level 5

6.1 Description

Level 5 of the Framework includes:

- A comprehensive security program that is an integral part of an agency's organizational culture.

- Decision-making based on cost, risk, and mission impact.

The consideration of IT security is pervasive in the culture of a level 5 asset. A proven life-cycle methodology is implemented and enforced and an ongoing program to identify and institutionalize best practices has been implemented. There is active support from senior management. Decisions and actions that are part of the IT life cycle include:

- Improving security program
- Improving security program procedures
- Improving or refining security controls
- Adding security controls
- Integrating security within existing and evolving IT architecture
- Improving mission processes and risk management activities

Each of these decisions result from a continuous improvement and refinement program instilled within the organization. At level 5, the understanding of mission-related risks and the associated costs of reducing these risks is considered with a full range of implementation options to achieve maximum mission cost-effectiveness of security measures. Entities should apply the principle of selecting controls that offer the lowest cost implementation while offering adequate risk mitigation, versus high cost implementation and low risk mitigation. The criteria listed below should be used to assess whether a specific control contained in the NIST questionnaire has been fully implemented.

6.2 Criteria

Level 5 criteria describe components of a fully integrated security program.

Criteria for Level 5
a. There is an active enterprise-wide security program that achieves cost-effective security.
b. IT security is an integrated practice within the asset.
c. Security vulnerabilities are understood and managed.
d. Threats are continually re-evaluated, and controls adapted to changing security environment.
e. Additional or more cost-effective security alternatives are identified as the need arises.
f. Costs and benefits of security are measured as precisely as practicable.
g. Status metrics for the security program are established and met.

7. Future of the Framework

This version of the Framework primarily addresses security management issues. It describes a process for agencies to assess their compliance with long-standing basic requirements and guidance. With the Framework in place, agencies will have an approach to begin the assessment process. The NIST questionnaire provides the tool to determine whether agencies are meeting these requirements and following the guidance.

The Framework is not static; it is a living document. Revisions will focus on expanding, refining, and providing more granularity for existing criteria. In addition, the establishment of a similar companion framework devoted to the evolution of agency electronic privacy polices may be considered in time.

The Framework can be viewed as both an auditing tool and a management tool.
A balance between operational needs and cost effective security for acceptable risk will need to be made to achieve an adequate level of security.

Currently, the NIST self-assessment tool is under development and will be available in 2001. Appendix A provides a sample questionnaire to assist agencies until NIST officially releases the questionnaire.

Appendix A
Conceptual Sample of NIST Self-Assessment Questionnaire

Below is a conceptual sample of the Hypothetical Government Agency's (HGA) completion of the NIST questionnaire for their Training Database. Before the questionnaire was completed, the sensitivity of the information stored within, processed by and transmitted by this asset was assessed. The premise behind determining the level of sensitivity is that each asset owner is responsible for determining what level of risk is acceptable, and which specific security controls are necessary to provide adequate security.

The sensitivity of this asset was determined to be high for confidentiality and low for integrity and availability. The confidentiality of the system is high due to the system containing personnel information. Employee social security numbers, course lists, and grades are contained in the system. The integrity of the database is considered low because if the information were modified by unauthorized, unanticipated or unintentional means, employees, who can read their own training file, would detect the modifications. The availability of the system is considered low because hard copies of the training forms are available as a backup.

The questionnaire was completed for the database with the understanding that security controls that protect the integrity or availability of the data did not have to be rigidly applied. The questionnaire contains a field that can be checked when a risk-based decision has been made to either reduce or enhance a security control. There may be certain situations where management will grant a waiver either because compensating controls exist or because the benefits of operating without the control (at least temporarily) outweigh the risk of waiting for full control implementation. Alternatively, there may be times where management implements more stringent controls than generally applied elsewhere. In the example provided the specific control objectives for personnel security and for authentication were assessed. The questionnaire is an excerpt and by no means contains all the questions that would be asked in the area of personnel security and authentication. For brevity, only a few questions were provided in this sample.

An analysis of the levels checked determined that the agency should target improving their background screening implementation and testing. System administrators, programmers, and managers should all have background checks completed prior to accessing the system. The decision to allow access prior to screening was made and checked in the *Risk Based Decision Made* box. Because this box was checked, there should be specific controls implemented to ensure access is not abused, i.e., access is reviewed daily through audit trails, and users have minimal system authority.

Additionally, HGA should improve implementing and testing their password procedures because of the strong need for confidentiality. Without good password management, passwords can be easily guessed and access to the system obtained. The questionnaire's list of objectives is incomplete for both personnel security controls and for authentication controls. Even though the sample is lacking many controls, the completed questionnaire clearly depicts that HGA has policies and procedures in place but there is a strong need for implementing, testing, and reviewing the procedures and controls. The sample indicates that the Training Database would be at level 2.

Hypothetical Government Agency's Backbone Local Area Network

Category of Sensitivity	Confidentiality	Integrity	Availability
High	X		
Medium			
Low		X	X

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made
Personnel Security						
Are all positions reviewed for sensitivity level?	X	X	X			
Is appropriate background screening for assigned positions completed prior to granting access?	X	X				X
Are there conditions for allowing system access prior to completion of screening?	X	X				
Are sensitive functions divided among different individuals?	X	X	X			
Are mechanisms in place for holding users responsible for their actions?	X	X				
Are termination procedures established?	X	X				
Authentication						
Are passwords, tokens, or biometrics used?	X	X	X			
Do passwords contain alpha numeric, upper/lower case, and special characters?	X	X				
Are passwords changed at least every ninety days or earlier if needed?	X	X				
Is there guidance for handling lost and compromised passwords?	X	X				
Are passwords transmitted and stored with one-way encryption?	X	X				
Is there a number of invalid access attempts that may occur for a given user?	X	X				

References

Automated Information Systems Security Program Handbook (Release 2.0, May 1994), Department of Health and Human Services, May 1994.

Clinger-Cohen Act of 1996 (formerly known as the Information Management Reform Act), February 10, 1996.

Computer Security Act of 1987, 40 U.S. Code 759, (Public Law 100-235), January 8, 1988.

Control Objectives for Information and Related Technology (COBIT) 3rd Edition, Information Systems Audit and Control Foundation, July 2000.

General Accounting Office, Federal Information System Control Audit Manual (FISCAM), GOA/AIMD-12.19.6, January 1999.

General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, GAO/AIMD-99-139, August 1999.

Office of Management and Budget, Security of Federal Automated Information Resources, Appendix III to OMB Circular A-130, Management of Federal Information Resources, February 8, 1996.

Office of Management and Budget, Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, Privacy and Personal Information in Federal Records, July 1, 1999.

Office of Management and Budget, Memorandum 99-18, Privacy Policies on Federal Web Sites, June 2, 1999.

Office of Management and Budget, Memorandum 00-13, Policies and Data Collection on Federal Web Sites, June 22, 2000.

Paperwork Reduction Act of 1995, 35 U.S. Code 44, January 4, 1995.

Presidential Decision Directive 63, Protecting America’s Critical Infrastructures, May 22, 1998.

Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government, October 21, 1998.

Swanson, Marianne and Barbara Guttman, NIST Special Publication 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP), Gaithersburg, MD, National Institute of Standards and Technology, September 20, 1995.

Swanson, Marianne and Federal Computer Security Program Managers' Forum Working Group, NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, Gaithersburg, MD, National Institute of Standards and Technology, December 1998.

Terminology

Acceptable Risk is a concern that is acceptable to responsible management, due to the cost and magnitude of implementing controls.

Accreditation is synonymous with the term **authorize processing**. Accreditation is the authorization and approval granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security. See also ***Authorize Processing, Certification,*** and ***Designated Approving Authority.***

Asset is a major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems.

Authorize Processing occurs when management authorizes in writing a system based on an assessment of management, operational, and technical controls. By authorizing processing in a system the management official accepts the risks associated with it. See also ***Accreditation, Certification,*** and ***Designated Approving Authority.***

Availability Protection requires backup of system and information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time-share systems, mission-critical applications, time and attendance, financial, procurement, or life-critical.

Awareness, Training, and Education includes (1) awareness programs set the stage for training by changing organizational attitudes towards realization of the importance of security and the adverse consequences of its failure; (2) the purpose of training is to teach people the skills that will enable them to perform their jobs more effectively; and (3) education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in IT security.

Certification is synonymous with the term **authorize processing.** Certification is a major consideration prior to authorizing processing, but not the only consideration. Certification is the technical evaluation that establishes the extent to which a computer system, application, or network design and implementation meets a pre-specified set of security requirements. See also ***Accreditation*** and ***Authorize Processing.***

General Support System is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

Individual Accountability requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

Information Owner is responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains that responsibility even when the data/information are shared with other organizations.

Major Application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

Material Weakness or ***significant weakness*** is used to identify control weaknesses that pose a significant risk or a threat to the operations and/or assets of an audited entity. "Material weakness" is a very specific term that is defined one way for financial audits and another way for weaknesses reported under the Federal Managers Financial Integrity Act of 1982. Such weaknesses may be identified by auditors or by management.

Networks include communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network or wide area networks, including public networks such as the Internet.

Operational Controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

Policy a document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.

Procedures a document that focuses on the security control areas and management's position.

Risk is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Risk Management is the ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Rules of Behavior are the rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal government equipment, assignment and limitation of system privileges, and individual accountability.

Sensitive Information refers to information whose loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs or the privacy to which individuals are entitled.

Sensitivity an information technology environment consists of the system, data, and applications that must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and/or availability which is determined by an evaluation of the sensitivity of the information processed, the relationship of the system to the organizations mission, and the economic value of the system components.

System is a generic term used for briefness to mean either a major application or a general support system.

System Operational Status is either (1) Operational - system is currently in operation, (2) Under Development - system is currently under design, development, or implementation, or (3) Undergoing a Major Modification - system is currently undergoing a major conversion or transition.

Technical Controls consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

Threat is an event or activity, deliberate or unintentional, with the potential for causing harm to an IT system or activity.

Vulnerability is a flaw or weakness that may allow harm to occur to an IT system or activity.