NISTIR 7328

Security Assessment Provider Requirements and Customer Responsibilities:

Building a Security Assessment Credentialing Program for Federal Information Systems

Arnold Johnson
Pat Toth

I N F O R M A T I O N S E C U R I T Y

INITIAL PUBLIC DRAFT

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2007

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
James M. Turner, Acting Director

Notes to Reviewers

The purpose of NIST Interagency Report (NISTIR) 7328, *Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program*, is to: (i) identify an initial set of requirements security assessment providers should satisfy to effectively conduct information system security control assessments in accordance with NIST Special Publication 800-53A, and (ii) facilitate a community dialog about these requirements.

The use of competent security assessment providers leads to more cost-effective and consistent results from the assessment process, which, in turn, provides more reliable results for authorizing officials to make informed, risk-based decision on the initial, or for continuing, operation of an information system.

This report also identifies some of the customer's responsibilities in providing an effective and cooperative environment in which security assessments can take place, and in adequately preparing for security assessments. Adequate preparation is an important aspect in conducting effective security assessments, and this report is intended to serve as a catalyst for dialog on this aspect of assessments as well.

A security assessment provider can demonstrate its capability to provide security assessment services by satisfying requirements in two areas:

- **Organizational management capability**[1] that each security assessment provider should have to effectively manage and operate a security assessment service; and
- **Security assessment capability** that each security assessment provider should have to effectively plan for, conduct, and document security assessments of information systems.

In 2006, NIST conducted a public workshop to introduce and solicit feedback on the ideas and options for a security assessment credentialing program and the potential requirements that security assessment providers should meet. The workshop presentations and a summary of the three workshop breakout sessions can be found at the NIST FISMA Implementation Project website http://csrc.nist.gov/groups/SMA/fisma/library.html.

General information about the FISMA Implementation Project, including all of the FISMA-related security standards and guidelines, how the FISMA publications can be used to manage enterprise risk and build a comprehensive information security program, and the organizational credentialing program under development as part of Phase II, can be found on the main web site at http://csrc.nist.gov/sec-cert.

Comments on NISTIR 7328 are requested by November 30, 2007. Comments should be forwarded to the Computer Security Division, Information Technology Laboratory at NIST or submitted via email to sec-cert-p2@nist.gov.

[1] Organizational management capability as used herein is the implementation of a management system that sufficiently enables service providers to manage, plan, conduct, and assure quality. A management system as defined by ISO9000:2005 Quality management systems — Fundamentals and vocabulary, is a set of interrelated or interacting elements to establish policy and objectives and to achieve those objectives. A management system of an organization can include different management systems, such as a quality management system, a financial management system or an environmental management system.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof-of-concept implementations, and technical analyses to advance the development and productive use of information technology. ITL responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The NIST Interagency Reports (NISTIR) provide information on ITL research, guidelines, and outreach efforts in information system security, as well as its collaborative activities with industry, government, and academic organizations.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. However, it may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

NIST Interagency Report 7328, 51 pages

(September 2007) CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

THE PUBLIC COMMENT PERIOD FOR THIS DOCUMENT IS OCTOBER 1 - NOVEMBER 30, 2007.

COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, INFORMATION TECHNOLOGY LABORATORY, NIST, SUBJECT: COMMENTS ON REQUIREMENTS FOR SECURITY ASSESSMENT PROVIDERS, VIA ELECTRONIC MAIL AT SEC-CERT-P2@NIST.GOV OR VIA REGULAR MAIL AT 100 BUREAU DRIVE (MAIL STOP 8930) GAITHERSBURG, MD 20899-8930

Acknowledgements

The authors Arnold Johnson and Pat Toth wish to thank Robin Medlock, Karen Quigg, and Elizabeth Foreman, Stu Katzke, Ron Ross, and Gary Stoneburner, who reviewed the document drafts and contributed to its development. A special note of thanks goes to Peggy Himes for her superb technical editing and administrative support and to and Carmella Thompson for her review of the document and insightful recommendations. The authors also gratefully acknowledge and appreciate the many contributions from individuals whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Table of Contents

CHAPTER ONE

INTRODUCTION

THE NEED TO VALIDATE CAPABILITIES FOR EFFECTIVE SECURITY ASSESSMENTS

The selection of a security assessment provider is a critical decision that customers of security assessment services must make. Security assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits—rather, they are the last line of defense in knowing the strengths and weaknesses of an organization's information system that is supporting critical applications and missions in a global environment of sophisticated threats. Security assessment providers should be prepared to provide effective and efficient assessments so that customers have reliable information to make decisions for authorizing information system operation, managing the information systems, and maintaining an adequate level of security for those systems.

An effective security assessment requires the cooperation and collaboration among all parties having a vested interest in the information system security posture. Establishing an appropriate set of expectations before, during, and after the security assessment is paramount to achieving a good outcome—that is, the assessment producing the information necessary for the authorizing official to make a credible, risk-based decision on whether to place the information system into initial operation or continue its current operation.

Thorough preparation by both the customers of the security assessment services and the assessment team that performs those services is an important aspect of conducting effective security assessments. The customer sets the stage for the success of the assessment by incorporating security into the system development life cycle[2] (SDLC), completing the steps in the National Institute of Standards and Technology (NIST) Risk Management Framework[3], having the appropriate security documentation completed and available, identifying the appropriate security personnel and officials, and making them available during the assessment. The assessment team should incorporate the information provided by the customer into a security assessment plan, develop effective assessment procedures, conduct the assessment, and document the findings following the standards and guidelines in applicable NIST publications.

1.1 Purpose and Applicability

The purpose of this report is to stimulate discussion and comments on the minimum capabilities security assessment providers should have to provide thorough and effective security assessment services. Based on comments and feedback received, NIST will update and republish this report for use as a reference in further development of a credentialing program for security assessment providers. Further, it is expected that the security assessment provider capabilities defined herein can be incorporated into statements of work as needed for acquiring security assessment services.

The report also identifies responsibilities of the customer in supporting security assessment providers that is necessary for making the security assessment a success. The success of the assessment process is dependent on the partnership and cooperation of these two groups.

[2] See Appendix D for a summary of the security related activities of the SDLC.

[3] See Appendix E for a description of the NIST Risk Management Framework.

One of the more difficult decisions facing a customer needing security assessment services, whether from an internal security team or from a third-party provider of the services, is determining if the security assessment provider and assigned assessment team possesses the competence and capability to adequately assess the security controls in the information system. To aid federal agencies in selecting adequate security assessment services, NIST is establishing a program for credentialing security assessment providers. The term credentialing as used herein is the process followed by security assessment providers in demonstrating competence for assessing information system security controls consistent with customer needs in implementing FISMA legislation, OMB policies, and NIST standards and guidelines. At this time the form, structure and concept of operations for a credentialing program has not been fully defined. The feedback on this report and from future workshops and other venues will be used to evaluate customer's requirements for a credentialing program. This information will be used to further define the credentialing program and program model.

The credentialing program will help make the security assessment provider selection process more reliable, leading to more informative security assessments and enabling greater validity for the risk decisions authorizing officials are required to make regarding the operation of information system. The credentialing program has the following objectives:

- Provide customers with a level of confidence that security assessment providers are qualified and capable of providing the requested services;
- Provide customers with an exemplary set of requirements that they can draw upon in developing specifications for acquisition of security assessment services;
- Provide security assessment providers with a basic set of requirements for use in developing corporate strategies to cost-effectively respond to customer requests for security assessment services;
- Enable more consistent and competent security assessment services from assessment teams resulting in more reliable assessment results that provide the basis for trust among interconnecting organizations;
- Enable more consistent, comparable, and cost-effective security assessments;
- Establish and maintain a registry of credentialed security assessment providers for customers that need assistance in performing security assessment services;
- Draw upon, when appropriate and applicable, international standards for defining accreditation and certification body[4] requirements in establishing a credentialing program[5];
- Ensure that credentialed security assessment providers maintain their organizational competencies through professional certifications, training programs, and continuing education; and
- Define customer responsibilities to adequately prepare for the security assessment and to provide a basic level of support that security assessment providers can expect from the customer organization for planning and conducting security assessments.

[4] ISO/IEC 17011, 17012, 17021 and 27006:2007 international standards refer to accreditation bodies as the entities that accredit certification bodies to conduct assessment / inspection services.

[5] The use of international standards in a credentialing program for federal information systems is intended to enable wider recognition of security assessment processes and assessment results for customer's information systems that may also require compliance with similar security controls (e.g., ISO 27001, HIPAA).

The credentialing program is being implemented in stages so potential participants in the program have the opportunity to provide feedback on the capability requirements planned for the program. This feedback will validate whether the basic elements of the program meet the needs of the various communities involved or indicate how the program can be modified to be more effective.

1.2 Target Audience

This report is intended to serve a diverse audience including:

- Organizations that provide security assessment services to customers (e.g., public or private sector organization responsible for conducting the security assessment);
- Individuals with information system and security assessment and monitoring responsibilities (e.g., assessors or assessment teams, system evaluators, certification agents, independent verification and validation assessors, auditors, inspectors general, information system owners);
- Individuals with information security implementation and operational responsibilities (e.g., information system owners, mission/information owners, and information system security officers); and
- Individuals with information system and security management and oversight responsibilities (e.g., authorizing officials, senior agency information security officers, information security managers).

1.3 FISMA Implementation Project

The Federal Information Security Management Act of 2002 (FISMA)[6] requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

In support of FISMA, NIST established the FISMA Implementation Project. The project is composed of two phases:

- Phase I: Security Standards and Guidelines Development; and
- Phase II: Organizational Credentialing Program.

Phase I

FISMA tasked NIST to develop standards, guidelines, and associated methods and techniques to aid federal agencies in securing their information systems. The standards and guidelines developed in Phase I include the following:

- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004;

[6] The E-Government Act (P.L. 107-347), passed by the one hundred and seventh Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006;
- NIST Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006;
- NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002;
- NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004;
- NIST Special Publication 800-39, *Managing Enterprise Risk A Framework for Addressing Cyber Threats to Organizations, Individuals, and the Nation* (projected for publication October 2007)*;*
- NIST Special Publication 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, December 2006;
- NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, Third Public Draft, June 2007;
- NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003; and
- NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, January 2004.

Phase II

The second phase of the FISMA Implementation Project focuses on the development of a program for credentialing public and private sector organizations to provide security assessment services. Security assessment services involve the comprehensive assessment of the management, operational, and technical security controls in federal information systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The assessments may be part of an information system certification and accreditation effort, in support of continuous monitoring of security controls, or for other types of information system security assessments.

Organizations that participate in the credentialing program need to demonstrate competence in the application of the NIST security standards and guidelines and the information security practices consistent with FISMA and OMB requirements. Developing a network of credentialed organizations with demonstrated competence in the provision of security assessment services will give federal agencies and other customers of security assessment services greater confidence in the acquisition and use of such services.

To help make security assessments more productive NIST is developing the Information Security Automation Program (ISAP) and the Security Content Automation Protocol (SCAP) suite of standards and content to facilitate faster, more reliable, and more cost-effective assessments of the security controls employed within information systems. ISAP strives to improve the security of information systems by identifying and reducing the number of known vulnerabilities and misconfigurations. The program automates the implementation of information system security controls through security data sharing in standard formats. SCAP is the public repository of security content to be used for automating technical control compliance activities, vulnerability checking (both application misconfigurations and software flaws), and security measurement.

ISAP facilitates the adoption of SCAP by government agencies, other organizations that conduct security assessments, and security vendors.

1.4 Security Assessment Process

Federal agencies are required to assess the effectiveness of the security controls that they have implemented in their information systems: (i) in a certification and accreditation of the information system before the system is approved for operation; and (ii) in assessments of security controls as part of the continuous monitoring process. Security assessments are typically conducted by information systems developers, systems integrators, certification agents, information system owners, auditors, inspectors general, and the information security staffs of security assessment provider organizations.

Assessment teams bring together available information about the information system such as the results from product-level assessments, if available, and conduct system-level assessments using a variety of methods and techniques defined in NIST Special Publication 800-53A. The assessments are used to compile and evaluate the evidence needed by information system owners and authorizing officials to determine how effective the security controls employed in the information system are likely to be in mitigating risks to organizational operations and assets, to individuals, to other organizations, and to the nation. The results from assessments conducted using assessment procedures derived from the guidelines in NIST Special Publication 800-53A, contribute to compiling the necessary evidence to determine security control effectiveness in accordance with stated requirements in NIST Special Publication 800-53.

In preparing for the security assessment, the information system security plan is reviewed, updated as needed, and approved by key organizational officials. The determination that the appropriate set of security controls has been selected and documented is part of the system security plan approval process that takes place before the security assessment begins. The assessment team reviews the system security plan for a description of the information system and the security controls planned for the system. If any discrepancies are found, the assessment team reports them to an appropriate official with a recommendation that the plan be amended as appropriate.

The availability of essential documentation as well as access to key organizational personnel and the information system being assessed are paramount to a successful assessment of the security controls. In preparation for the assessment of the security controls, the necessary background information should be assembled and made available to the assessment team. The customer should identify and arrange access to: (i) individuals or groups responsible for the development, implementation, operation, and maintenance of security controls; (ii) any material (e.g., system security plans, records, schedules, assessment reports, after-action reports, agreements, accreditation packages, interconnection agreements, security policies and implementation procedures) associated with the implementation and operation of security controls; and (iii) the objects to be assessed.

The assessment team develops the security assessment plan that provides the objectives for the security control assessment, the roadmap of how to conduct the assessment, and the detailed assessment procedures for testing each security control. The security assessment procedures are applied to determine if the agreed-upon and approved security controls are in fact, implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

Figure 1 provides an overview of the security assessment process that is employed to determine security control effectiveness.

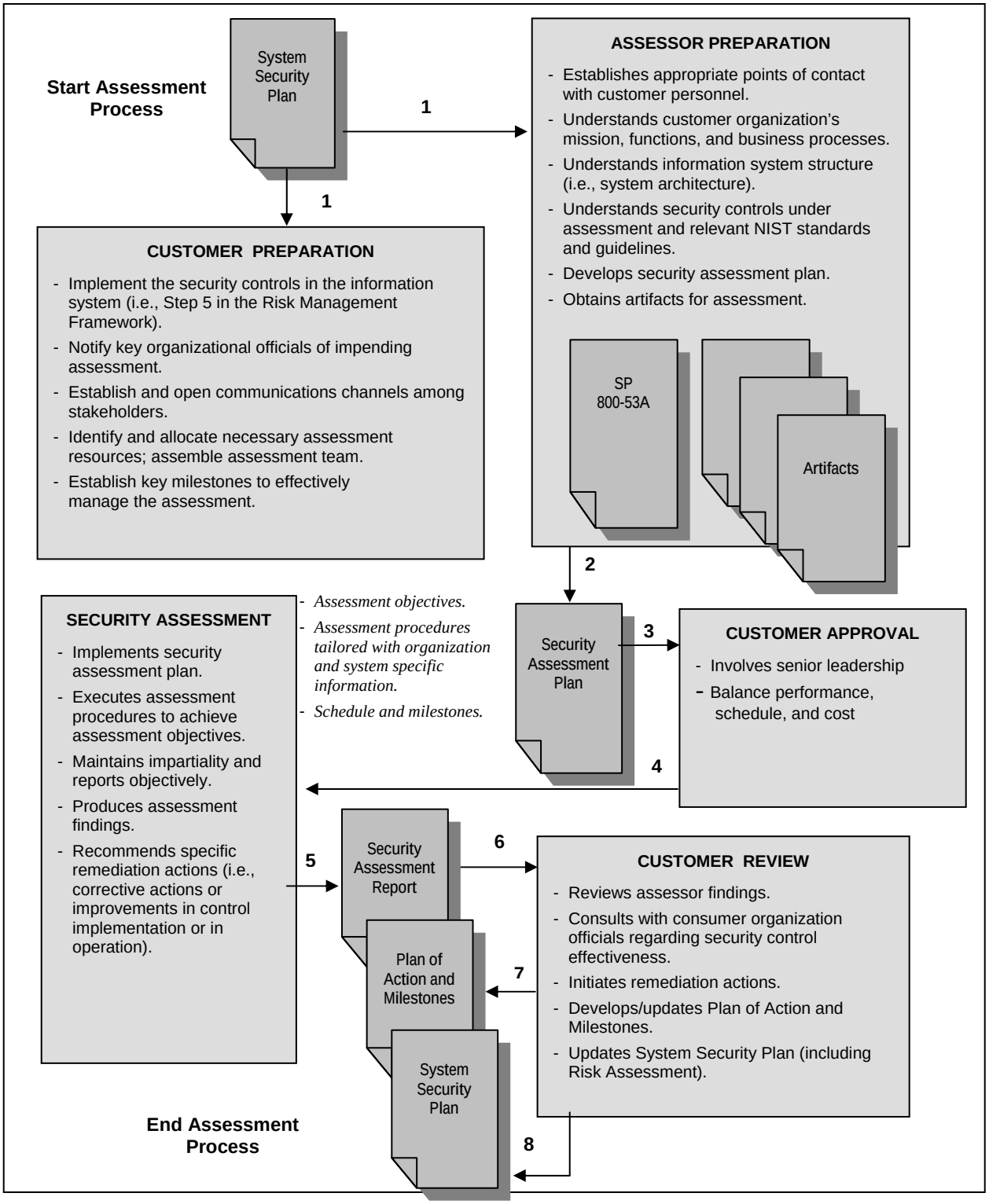

FIGURE 1: SECURITY ASSESSMENT PROCESS OVERVIEW

The output of the security assessment is the security assessment report, which documents the results of the assessment. The security assessment report includes information in the form of assessment findings necessary to determine the effectiveness of the security controls employed in the information system. The report is a key factor in the authorizing official's determination of risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation.

The assessment findings produced by the assessment team are provided to the information system owner. The information system owner reviews the findings of the assessment team and coordinates with other organizational officials to determine and document the appropriate steps to correct weaknesses and deficiencies identified during the assessment.

1.5 Roles in Security Assessment

The following sections describe the roles of the key participants associated with the security assessment effort. While organizations that use these guidelines may associate other names with these roles, their basic functions and responsibilities remain the same. Table 1 identifies the key participants in the assessment process and the expectations related to their involvement.

TABLE 1: SECURITY ASSESSMENT ROLES

Role	Expectation
NIST	• Develop information system security standards and guidelines • Establish credentialing program for security assessment provider organizations • Define training guidelines to support the credentialing program
Security Assessment Customers	• Prepare for the assessment • Approve security assessment plan prior to executing the assessment • Provide enterprise perspective
Security Assessment Providers	• Provide internal support structures for assessment teams • Organize teams with complementary skills • Have internal procedures in place to provide consistent and repeatable services • Maintain independence from developmental and implementation processes • Assess the security controls and document the assessment findings

NIST

NIST develops standards and guidelines consistent with its responsibility for supporting federal agencies in the implementation of FISMA including the assessment of security controls. NIST will define training guidelines to aid security assessment providers and customers in the use of NIST standards and guidelines that will enable organizations and individuals to gain the basic knowledge to effectively conduct security assessments. As the credentialing program progresses through later phases, NIST will further define its oversight responsibilities for the credentialing program.

Security Assessment Customers

Customers are organizations that acquire security assessment services (e.g., federal agencies; state, local, or tribal governments; private sector organizations that comprise the critical infrastructure of the United States; commercial companies that follow NIST standards and guidelines). Customers define what needs to be assessed, complete their preparation tasks prior to the assessment, and share the information with the assessment team. Customers can acquire services through a contractual relationship or internally through an agreement with another part of the customer's organization or another organization.

Within the customer's organization, the authorizing official and system owner are responsible for evaluating the assessment findings and determining the appropriate actions that should be taken to address any identified weaknesses or deficiencies. The authorizing official formally accepts the risk and assumes the responsibility for operation of the information system based on the security assessment results and other information.

Security Assessment Providers

A security assessment provider is a public or private sector organization responsible for conducting the security assessment and is expected to select appropriate assessment teams with individuals containing the combination of knowledge, skills, and abilities to conduct each assessment. The provider should have the management structure and standard operating procedures to effectively manage the assessment process and the individuals assigned to the assessment team.

The assessment team is responsible for conducting a comprehensive assessment of the management, operational, and technical security controls in an information system. To preserve the impartial and unbiased nature of the security assessment the security assessment provider and each member of the assessment team should be in a position that is independent from the persons directly responsible for the development of the information system and the day-to-day operation of the system.

1.6 Organization of This Document

The remainder of this NIST Interagency Report (NISTIR) is organized as follows:

- **Chapter Two** describes the responsibilities that customers have in making the security assessment process a success;
- **Chapter Three** describes the capabilities that security assessment providers should have to be deemed competent to participate in the credentialing program. The security assessment provider organizes teams that together have the necessary knowledge, skills, and abilities to conduct an effective security assessment; and
- **Supporting appendices** provide more detailed information related to the credentialing program including: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) a description of the security-related activities during the SDLC[7]; (v) a description of the NIST Risk Management Framework; (vi) a readiness review checklist to validate that the customers are ready for the security assessment; and (vii) a validation checklist that can be used by customers to validate that a security assessment provider has met the expected capabilities to conduct the security assessment or by security assessment providers to demonstrate they have the capabilities to conduct an effective security assessment.

[7] See Appendix D for a summary of the security related activities that comprise each phase of the SDLC.

CHAPTER TWO

SECURITY ASSESSMENT CUSTOMERS

RESPONSIBILITIES FOR SUPPORTING SECURITY ASSESSMENTS

Customer's preparation and support for the security assessment is an important aspect of conducting effective security assessments. This chapter focuses on the responsibilities of the customer in preparing for and supporting the security assessment. To validate that the customer has completed the recommended activities prior to the assessment, the customer should conduct a readiness review. The readiness review provides an important function in verifying that the necessary activities have been completed, documentation has been prepared and collected, and appropriate people have been identified and notified of potential interviews. Completing the readiness review and compiling the materials into a logical arrangement allows the customer to quickly provide the information necessary to the security assessment team so the team can complete the preparation activities and document them in the security assessment plan. A readiness review checklist is included in Appendix F.

In addition to being prepared for each information system security assessment, having a strong enterprise-wide security program provides a foundation for understanding and implementing security effectively throughout the customer's organization. The enterprise-wide strategy should begin by applying the initial components of the NIST Risk Management Framework[8] to all information systems within the customer's organization with an enterprise view of the security categorization process, the security control selection process, and the identification of common security controls[9]. Customers should have adequate security policies and procedures, knowledge, tools, and techniques in place for assessment teams to perform the security assessments in an efficient and cost-effective manner. Customers should also ensure that information security is addressed from information system initiation to disposition. Including security early in the SDLC[10] process results in less expensive and more effective security implementation.

The identification of common security controls is most effectively accomplished as an organization-wide exercise with the involvement of senior security officials. Partitioning security controls into common controls and system-specific controls can result in significant savings to the organization in development and implementation costs especially when common controls serve multiple information systems and entities. An organization-wide approach to reuse and sharing of assessment results can greatly enhance the efficiency of the security assessments being conducted and significantly reduce security program costs.

An enterprise-wide approach to developing and implementing security document templates (e.g., system security plan, contingency plan, and incident response plan) or the selection of tools that support the security assessment process establishes expectations for security assessment documents and leads to greater consistency in the customer organization's approach to security assessments. Providing security document templates for the customer's organization establishes clear expectations about what is required for each document, including the topics in the document

[8] See Appendix E for a description of the NIST Risk Management Framework.

[9] Common security controls are controls that can be applied to: (i) one or more organizational information systems; (ii) a group of information systems at a specific site; (iii) common information systems, subsystems, or applications (i.e., common hardware, software, or firmware) deployed at multiple operational sites. See NIST Special Publication 800-53 for a more complete description of common security controls.

[10] See Appendix D for a summary of the security related activities that comprise each phase of the SDLC.

and the level of detail that should be included. In turn, this provides greater consistency to the entire security assessment process.

Automated tools are important to support the security assessment process, each with a different focus and capabilities. As customer organizations have the resources necessary to acquire and implement available automated tools, the customer organization further simplifies the security assessment process and enables a more consistent implementation and validation of information obtained through the assessment process. Customer organizations that have their own assessment tools or security document templates are expected to provide training to the assessment teams so that the tools and templates are used consistently and effectively.

An effective information security program should also include an aggressive continuous monitoring program to check the status of the security controls in the information system on an ongoing basis. The ultimate objective of the continuous monitoring program is to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system as well as the environment in which the system operates. An effective continuous monitoring program requires an established configuration management and control change processes for the information system, where the security impact of the requested change is analyzed, assessed as necessary, and reported to the appropriate consumer officials.

2.1 Maintain Independence from Assessment Team

The customer may require an independent security assessment. Independent security assessment services can be obtained from other elements within the customer's organization or can be contracted to a public or private sector entity outside of the customer's organization. Contracted assessment services are considered independent if the information system owner cannot unduly influence the independence of the assessment team conducting the assessment of the security controls in the information system. The authorizing official determines if the level of assessment team independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision.

2.2 Prepare for Security Assessment

Preparation by the customer is an important aspect of conducting effective security assessments. Preparatory activities should address a range of issues related to the cost, schedule, and performance of the security assessment.

Establish expectations for the security assessment—

The customer should begin by establishing the objective and scope of the security assessment—they should identify what is being assessed and what is necessary to achieve the objectives. Based on the objective and scope, the customer determines the level of effort and resources (e.g., size and organizational characteristics of the assessment team—skill sets, technical expertise, and assessment experience of individuals composing the team) needed to carry out the security assessment. The customer establishes the time frame necessary for completing the assessment and the key milestone decision points for effectively managing the assessment. The customer should allow sufficient time and resources for the security assessment provider to complete the requirements required for the contracting process (e.g., security awareness training, security background investigation paperwork and processing, or connection requirements for accessing the customer's information systems).

All key organizational officials should be notified of the impending security assessment, establishing appropriate communication channels within the customer organization. The customer and the assessment team should also establish an effective communications mechanism to minimize ambiguities or misunderstandings. Communications should be initiated at an orientation meeting, maintained through on-going task meetings, and concluded at the final close-out meeting.

Perform a readiness review for the security assessment—

Prior to the orientation meeting, the customer should prepare for each information system security assessment. The readiness review checklist in Appendix F will help the customer identify and compile all necessary information and materials that they should provide to the security assessment team. The customer should confirm the following:

- The information system has been fully described and documented in the system security plan and/or supporting documentation (e.g., purpose, capabilities, operating environment, interconnections with other systems, user characteristics, and privileges);
- The information system security category has been determined and documented in the system security plan;
- Potential threats that could exploit information system flaws or weaknesses have been identified and documented in the risk assessment report or the system security plan;
- The security controls have been identified and their implementation documented in the system security plan;
- Common security controls have been assessed through an independent assessment (or independent validation of assessment results) and the results made available to the security assessment team;
- The risk to organizational operations and assets, individuals, other organizations, and the nation has been determined and documented in the risk assessment and/or system security plan; and
- All required security-related documents, records, and assurance evidence is completed and will be available for the assessment.

If the security assessment is being conducted as part of the information system certification and accreditation process, the customer should ensure that the system security plan has been approved by appropriate senior officials prior to initiating the security assessment.

If the security assessment is being conducted as part of continuous monitoring, a self-assessment, or annual FISMA evaluation, the customer is responsible for determining the subset of security controls that will be assessed.

Identify security and safety ground rules, and facilities for assessment team—

The customer should have adequate policies and procedures in place prior to the assessment that deal with handling of customer data during/after the assessment and communicate those policies to the security assessment provider.

The customer should also plan for administrative issues related to the security assessment. The customer should determine if the assessment team needs an escort during the assessment, and if so, identify the escort or group of escorts. If the assessment team will be working in the customer facilities, they will need appropriate office equipment. While most assessments take place in an office or data center environment, some assessments may take place in locations that require

special safety equipment or considerations. The safety conditions and any issues regarding handicap access should be identified and communicated to the security assessment provider. Special safety considerations such as working in static free areas requiring lab coats, grounding straps etc., the requirement for safety glasses, hard hats, steel toe shoes etc. restricted areas should be identified. If personnel conduct shift work that are needed for assessment objectives that are off cycle this should be identified and communicated to the security assessment provider.

2.3 Make Artifacts Available for Security Assessments

For security assessments to be timely and effective, assessment teams need to evaluate various information security-related documents and records developed for, or as result of the operation of, the information system. Therefore, it is imperative that customers ensure that these documents and records are complete and made available at the initiation of the security assessment process.

Among the artifacts that customers should identify, assemble, and make available to the assessment teams are:

Security policies and any associated implementing procedures;

Any materials (e.g., system security plans, system diagrams, risk assessments, contingency plans, incident response plans, assessment reports, after-action reports, current plans of action and milestones, interconnection agreements, and accreditation packages) associated with the implementation and operation of security controls;

Information system, which includes equipment, hardware, software, firmware, network, physical facilities, and interconnections with other systems;

Documentation, records, or other evidence, which may have been provided during the acquisition/development phase or the implementation phase of the system, associated with the implementation and operation of security controls;

Any assurance products or other evidence prepared during the assessment of common security controls; and

Any documentation, records, or other evidence related to the implementation of service-oriented architecture.

2.4 Make Personnel Available for Security Assessments

In conducting security assessments, assessment teams may need to interview agency individuals knowledgeable about the information system and the system's information security. Therefore, customers should identify and make available, at the places and times agreed upon with the assessment team, those individuals or groups within the organization who are responsible for implementing, operating, and maintaining the information system.

The assessment teams are expected to work with customer technical managers, such as the information system owner or the information system security officer, who are responsible for acquiring security assessment services and for developing and providing the required documentation for the information system being assessed. These managers are also responsible for developing a comprehensive plan of action and milestones based on security assessment findings. These managers are expected to have a detailed understanding of the risk management process and the technical requirements for information systems that are consistent with NIST standards and guidelines.

The assessment team may also need to interview individuals responsible for implementing the security controls and operating the information system. These individuals could include the developers of the information system, system administrators, database administrators, or web administrators. Many customer organizations group their applications together in large data centers. Individuals that manage and operate the data centers may need to be interviewed during the security assessment.

Assessment teams may also interact with customer senior officials who are responsible for establishing and funding information security programs within their organizations. Such officials may need to be contacted and interviewed because of their detailed understanding of the overall organizational-level risk management process, agency security program, and compliance with FISMA-related regulations and NIST standards and guidelines.

2.5 Approve Security Assessment Plan Prior to Assessment

Once the assessment team has completed the security assessment plan, the plan is reviewed and approved by the appropriate official in the customer organization to ensure that the plan is consistent with the security assessment objectives, their assessment of risk, and cost-effective with regard to the resources allocated for the assessment. After the security assessment plan is approved, the assessment team executes the plan in accordance with the agreed-upon milestones and schedule.

CHAPTER THREE

SECURITY ASSESSMENT PROVIDERS

CAPABILITY REQUIREMENTS FOR CONDUCTING EFFECTIVE SECURITY ASSESSMENTS

Conducting an effective security assessment is a process that involves: (i) compiling evidence that the security controls employed in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system; and (ii) presenting this evidence in a manner that decision makers are able to use effectively in making credible, risk-based decisions about the operation or use of the system. The evidence described above comes from both the implementation of the security controls in the information system and from assessments of that implementation.

Security assessments are typically conducted by information system developers, system integrators, certification agents, information system owners, auditors, inspectors general, and the information security staffs. The assessment teams bring together information available about the information system such as the results from product-level assessments, if available, and conduct additional system-level assessments using a variety of methods and techniques The results from previous assessments conducted using information system-specific and organization-specific assessment procedures derived from the guidelines in NIST Special Publication 800-53A contribute to compiling the necessary evidence to determine security control effectiveness in accordance with stated assurance requirements in NIST Special Publication 800-53.

Security assessment services, whether provided by an element within the customer's organization or a public or private sector entity contracted to provide services, should demonstrate a variety of different capabilities. The security assessment provider should have an appropriate management structure that provides the framework for assessment teams to conduct the security assessment. The security assessment provider should be able to perform administrative functions to support the assessment teams, protect the information received from the customer, and develop and implement standard procedures to ensure that all assessment teams provide consistent and reliable assessment services. Security assessment providers select appropriate individuals to make up an assessment team. The team member's should work together to prepare for, conduct, and document the findings of the assessment. Each team is made up of individuals that should collectively have the knowledge, skills, and abilities to conduct the security assessment. This chapter describes the requirements for security assessment providers in three areas—organizational, assessment teams, and individual knowledge, skills, and abilities.

Appendix G provides a checklist to validate that the security assessment provider has demonstrated the prerequisite capabilities necessary to conduct security assessments. The checklist can be used by the security assessment providers to establish their security assessment practices and to demonstrate their compliance with the expected capabilities. The checklist can also be used by customers when evaluating security assessment providers to validate that they have effectively demonstrated the capabilities expected.

3.1 Organizational Management Capability

Organizational management capability for a security assessment provider is the implementation of a management system that sufficiently enables a service provider to manage, plan, conduct and assure quality of security assessment services. The security assessment provider should have an

in place, operational and appropriate management system in order to effectively manage and conduct security assessments. The management system framework should include: (i) maintaining independence to prevent a conflict of interest when conducting the security assessments; (ii) implementing an effective management structure that provides both technical oversight and administrative support; (iii) providing the resources to select an effective assessment team with the knowledge, skills, and abilities to conduct the assessment based on the customer's information system environment; (iv) protecting customer information collected during the security assessment process; and (v) implementing or creating tools, templates, and standard security assessment procedures to ensure each assessment team provides a consistent standard of service. Customers should be confident that the security assessment provider security assessment teams have the knowledge, experience, and resources to conduct an effective security assessment.

3.1.1 Maintain Independence to Prevent Conflict of Interest

The independence of the assessment team is an important factor in assessing the credibility of the security assessment results, and ensuring the authorizing official receives the most objective information possible in order to make an informed, risk-based, accreditation decision. To preserve the impartial and unbiased nature of the security assessment, the assessment team should not be directly involved in:

- Development of the information system;
- Day-to-day operation of the system;
- Correcting security deficiencies; or
- Matters, activities or interests that could potentially influence the outcome of the assessment results

If the security assessment provider is providing other security services to a customer, the provider may also provide security assessment services as long as there is an adequate segregation of responsibilities and accountabilities between the sub-organizations that are providing the services. The provider's management should assign different individuals to provide oversight to the other security services separate from the security assessment services, validate that different personnel are assigned to security assessment services, validate that the personnel are not involved in authorization to operate decision-making, and ensure there is no possibility of influencing the outcome of the assessment.

3.1.2 Implement Management Structure to Support Security Assessments

The security assessment provider should implement and maintain an organizational structure that enables it to perform its technical functions satisfactorily and adequately conduct its administrative functions. In order to provide consistent services, the security assessment provider should have a technical manager that is a permanent employee, is qualified and experienced in providing security assessment services, and has overall responsibility for all security assessments performed within the security assessment provider's organization. This technical manager is not required to actively participate in all security assessments, but is expected to develop internal methods and procedures to enable all security assessors to provide consistent and reliable services. The technical manager should validate the quality of the products produced in support of the security assessment to ensure their consistency and that they meet the standards established by the security assessment provider. In addition, the technical manager is responsible for ensuring that all security assessors are adequately trained and that they have and maintain any required professional qualifications.

The security assessment provider should also have implemented adequate administrative functions in order to operate effectively. These administrative functions include the ability to contract for services, properly account for time and attendance, maintain accounts and financial records, obtain personnel, and maintain appropriate business records. The administrative functions should comply with all federal, state, and local laws and regulations.

3.1.3 Select Security Assessment Team

The technical manager selects individuals for each information system assessment that have the knowledge and experience necessary for the security assessment. The selected individuals should understand security control concepts and how the associated security controls are implemented in the information system. The assessment team collectively should be familiar with information security legislation, standards, and guidelines.

- In addition, team personnel should have:
- Relevant knowledge and training on security assessment methods and procedures;
- Relevant experience conducting security assessments; and
- Relevant experience with the technologies in the planned security assessment.

While each individual assigned to an assessment team does not need to have all the knowledge, skills, and abilities defined in section 3.3, the team should collectively have all the knowledge, skills, and abilities required for a successful security assessment. This allows team members to work together to accomplish the goals of the assessment, contribute their strengths to the team, and train individuals that are new to the assessment field.

3.1.4 Protect Customer Data

The assessment team may obtain information during a security assessment that the customer does not want to share with others. The security assessment provider has an obligation to safely and securely store and protect the confidentiality of all security assessment related records and information, including limiting access within their organization to the individuals that need to know the information. As part of the document control process, protection measures to ensure the confidentiality, integrity, and availability of the information should be consistent with legislation, regulations, and customer requirements. When transmitting information related to the security assessment with the customer, the security assessment provider should follow the guidelines established by the customer. The assessment provider organization should become familiar with and abide by these requirements.

3.1.5 Implement Standard Assessment Processes and Procedures

Security assessment providers range in size from one person operations, to large national/international corporations, to elements internal to the customer's organization. No matter the size of the organization, the customer should be assured that they will receive an equivalent quality of service regardless of the persons assigned to participate in the security assessment. The security assessment provider should create and maintain standard procedures on how to complete the security assessment, including checklists, document templates, and software tools to ensure a consistent quality among all assessors. These processes and procedures, and supporting templates and tools, should be consistent with NIST standards and guidelines. As the size of the security assessment provider organization increases, the need for automated tools to ensure the consistency of their assessment services increases.

Many customers have their own templates, tools, and security assessment procedures. The security assessment provider should be able to modify its approach to meet the needs and expectations of the customer. Security assessment providers should review the customer's tools, templates, and assessment procedures and if there is reason to believe that there are discrepancies that would adversely affect assessment of the security controls the assessment team should report those discrepancies to the customer and work with the customer to resolve the issues.

3.2 Security Assessment Team Capability

The security assessment provider selects team members to conduct the security assessment and provides them with the appropriate organizational structure and resources. The assessment team requirements include: (i) participating in the initial orientation meeting to gain the information necessary to conduct the assessment and validate that the customer organization is ready for the assessment; (ii) preparing the security assessment plan that is consistent with standards and guidelines and incorporates customer-specific requirements; (iii) conducting the assessment after all required approvals have been obtained; and (iv) documenting the findings in the security assessment report. The assessment team should collaborate, bringing together their diverse skills, to prepare for, conduct, and document the findings of the security assessment.

3.2.1 Participate in Orientation Meeting

At the initial orientation meeting with the customer the security assessment team, should gain an understanding of the customer's organization, the information system, and customer-specific tools, templates, and security assessment procedures. The customer should provide the results of the readiness review (Appendix F) and discuss the results with the team so that they will be able to plan and conduct the assessment efficiently and effectively. The assessment team reviews the readiness review to validate the customer is prepared for the security assessment and confirms the availability of the information, contacts, documents, and access to the information system needed to conduct the security assessment. The assessment team should validate that they have received the following:

- A general understanding of the organization's operations (including mission, functions, and business processes) and how the information system under assessment supports organizational operations;
- An understanding of the structure of the information system (e.g., system architecture) that is the subject of the security assessment;
- A thorough understanding of the security controls being assessed as approved in the system security plan;
- Appropriate organizational points of contact needed to carry out the security assessment;
- Artifacts needed for the security assessment (e.g., policies, procedures, specifications, designs, records, administrator/operator manuals, information system documentation, previous assessment results); and
- A realistic schedule to conduct the security assessment effort consistent with task assigned and the resources allocated to the assessment.

3.2.2 Develop Security Assessment Plan

The security assessment plan provides the objectives for and a detailed roadmap of how to conduct an assessment of the information system security controls. There are a series of distinct

steps[11] that the assessment team should follow in developing a plan to assess the security controls in the information system to include:

- Determine the type of security assessment and which security controls and control enhancements are to be included in the assessment;
- Select the appropriate assessment procedures to be used during the security assessment;
- Tailor the selected assessment procedures as appropriate to:
  - Select the assessment objects needed to make appropriate determinations and satisfy assessment objectives;
  - Assign depth and coverage attribute values in accordance with the assigned information system impact level;
  - Eliminate assessment procedures for common security controls if those controls have been assessed by another documented assessment process;
  - Develop information system/platform-specific and organization-specific extensions to provide the level of detail necessary to successfully carry out the assessment of the security controls;
  - Incorporate assessment results from previous assessments where the results demonstrate a sufficient coverage; and
  - Adjust assessment procedures to obtain the requisite assessment evidence from external providers.
- Develop additional assessment procedures, if necessary, to address security control and control enhancements that are not contained in NIST Special Publication 800-53, or to address additional assurance requirements beyond what is provided in NIST Special Publication 800-53A;
- Adjust the assessment procedures as appropriate to assess the security controls consistent with the life cycle phase[12];
- Develop a strategy to apply the extended assessment procedure(s);
- Optimize the assessment procedures to reduce duplication of effort and provide cost-effective assessment solutions; and
- Finalize the assessment plan and obtain the necessary approvals to execute the plan.

Assessment teams are responsible for obtaining the evidence necessary for customer officials to determine the effectiveness of the security controls in the organization's information system as documented in the system security plan. The assessment team should review the system security plan to ascertain whether or not the plan addresses all of the security controls selected for implementation during the baseline tailoring and supplementation process. If the assessment team finds any apparent discrepancies in the system security plan with regard to meeting the customer security requirements for the information systems based on FIPS 200 and NIST Special Publication 800-53, they should report the deficiencies to the appropriate customer officials for resolution.

[11] NIST Special Publication 800-53A describes the series of steps security assessors should consider when developing the security assessment plan.

[12] See Appendix D for a description of the security related activities that should be conducted during each SDLC phase

Most information systems are composed of a variety of components (hardware, software, firmware), with each component implementing some, but not all, of the security controls in the system. Each security control should be adequately assessed, which may require assessing the control multiple times on different components. Each component and the security controls assigned to the component should be identified by the assessment team. The assessment team tailors the security assessment procedures to address the specific environment in which the components are implemented. Based on the range of components that should be assessed, the assessment team develops a strategy to assess the components and their related security controls, ensuring that all security controls are assessed.

If there is a multiple number of the same component (e.g., desktop or laptop computers, firewalls, mail servers), the assessment team determines, in coordination with the customer, whether sampling can be effectively used in assessing the security controls. Sampling decisions and strategy should be documented in the security assessment plan.

3.2.3 Conduct Security Assessment

The security assessment provides the authorizing official with important information necessary to make credible, risk-based decisions on whether to place an information system into operation or continue its current operation. This information is obtained by assessing the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The security assessment follows the guidance in NIST Special Publication 800-53A, tailored to the customer's organizational environment as documented in the security assessment plan. The assessment is conducted using a variety of methods and associated assessment procedures depending on the depth and breadth of assessment required by the customer.

The security assessment methods are examine, interview, and test. The examine method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects to gain understanding, achieve clarification, or obtain evidence. The interview method is the process of conducting discussions with individuals or groups of individuals within the customer's organization to once again facilitate assessor understanding, achieve clarification, or obtain evidence. The test method is the process of exercising one or more assessment objects under specified conditions to compare actual with expected behaviors. In all three assessment methods, the results are used in making specific determinations called for in the determination statements and thereby achieving the objectives for the assessment procedure.

The technical tests are often supported by a variety of scanning tools appropriate for the information system environment. Assessors should be experienced with technical scanning tools and know when it is appropriate to use them. Examples of technical tests and scanning tools that may be used include: (i) network scanning tools; (ii) host-based tests, (iii) password checkers; (iv) host configuration audits; (v) database scanners; and (vi) web server vulnerability scanners.

3.2.4 Prepare Security Assessment Report

The assessment team compiles and analyzes the information collected during the assessment process and documents the findings in the security assessment report. The report should follow the guidelines in NIST Special Publication 800-53A or a customer specified report format. The security assessment report contains:

- Results of the security assessment (i.e., the determination of the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system); and
- Recommendations for correcting deficiencies in the security controls and reducing or eliminating identified vulnerabilities.

3.3 Assessment Team Knowledge, Skills, and Abilities

Assessment teams are made up of individuals that collectively have the knowledge, skills, and abilities to conduct security assessments. Assessment teams are expected to demonstrate competence in planning and conducting comprehensive assessments of the management, operational, and technical security controls in organizational information systems and in documenting the findings of the assessments in security assessment reports. These findings are used to support security decisions regarding operation of the information system, correcting deficiencies and in the continuous monitoring of security controls, and FISMA/OMB reporting.

While each team member does not need all the knowledge, skills, and abilities, the team collectively needs them to conduct each security assessment. Appendix V of the Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual* (FISCAM) provides the following definitions and examples of these terms:

- **Knowledge**—the foundation upon which skills and abilities are built. Knowledge is an organized body of information, factors, principles, or procedures which, if applied, makes adequate performance of a job possible. An example is knowledge of the tools and techniques used to establish logical access control over an information system;
- **Skill**—the proficient manual, verbal, or mental manipulation of people, ideas, or things. A skill is demonstrable and implies a degree of proficiency. As an example, a person may be skilled in using a software product to conduct an automated review of the integrity of an operating system; and
- **Ability**—the power to perform a job function while applying or using the essential knowledge. Abilities are evidenced through activities or behaviors required to do a job. An example is the ability to apply knowledge about logical access controls to evaluate the adequacy of an entity's implementation of logical access controls.

3.3.1 Assessment Team Knowledge Requirements

The knowledge requirements needed for assessments will vary based on the type of assessment and assessment environment. However, the selected assessment teams should have sufficient knowledge from experience or training in the following areas:

- Information technology specific to the information system and the technologies' functions;

- Software specifications (e.g., functional specification, high-level design, low-level design, and source code);
- Information system architecture (i.e., components and their interactions);
- Testing and assessment tools;
- Information technology security concepts, principles, analysis methods, and practices;
- SDLC phases and the security considerations in each phase;
- Information security roles and responsibilities;
- System security engineering principles and practices;
- FISMA and other federal laws' security-related requirements for federal departments and agencies (e.g., the Health Insurance Portability and Accountability Act of 1996, the Federal Financial Management Improvement Act of 1996, or OMB Circular A-127 on Financial Management Systems);
- OMB security-related circulars, policies, memoranda, and other directives;
- NIST's Information Security Automation Program (ISAP) and related Security Content Automation Protocols (SCAP);
- Security assessment reporting guidelines;
- NIST FIPS, minimally:
  - FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*; and
  - FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.
- NIST guidelines, minimally:
  - NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information System*;
  - NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*;
  - NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*;
  - NIST Special Publication 800-39, *Managing Enterprise Risk A Framework for Addressing Cyber Threats to Organizations, Individuals, and the Nation;*
  - NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*;
  - NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*;
  - NIST Special Publication 800-60: *Guide for Mapping Information and Information Systems to Security Categories;*
  - NIST Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*; and
  - NIST Special Publication 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers*.

Each assessment team member can gain knowledge of the assessment process, information technology products and services, and information security controls through education as demonstrated by an academic degree or certificate program. Additional

knowledge can be demonstrated through further professional certifications or product or technology specific certifications and training. Knowledge of the NIST Risk Management Framework provides the specific knowledge required to implement a security assessment program consistent with NIST standards and guidelines. Knowledge of the NIST Risk Management Framework can be demonstrated by obtaining a certificate of completion of a NIST-approved training program. The assessment team should be able to collectively demonstrate sufficient knowledge to cover all the minimum security requirement topics defined in FIPS 200, *Minimum Security Requirements for Federal Information Systems*,.

3.3.2 Assessment Team Skill Requirements

Security assessment teams should have the skills described below, which are gained from experience. The assessment procedures in NIST SP 800-53A require assessors to have at least five major skills (i.e., examine, interview, test, sampling, and penetration testing); the results of which are used to support the determination of overall security control effectiveness.

Examine

The examine skill consists of being proficient in checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, and activities) to facilitate understanding, achieve clarification, or obtain evidence—the results of which are used to determine a security control's existence, functionality, and potential for improvement.

Typical examinations may include reviewing information security policies, plans, and procedures; analyzing system design documentation and interface specifications; observing system backup operations; reviewing and analyzing the results of contingency plan exercises or drills; observing incident-response operations or activities; checking security configuration settings; checking, studying, or observing the operation of an IT mechanism in the system hardware/software; observing physical security measures related to system operation; or studying technical manuals and user/administrator guides.

Interview

The interview skill consists of being proficient in conducting focused discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence.

Typical interviews may include, for example, interviewing agency heads, chief information officers, senior agency information security officers, authorizing officials, information owners, information system and mission owners, information system security officers, information system security managers, personnel officers, human resource managers, facilities managers, training officers, information system operators, network and system administrators, site managers, physical security officers, and users.

Test

The test skill consists of being proficient in exercising one or more assessment objects under specified conditions to compare actual with expected behavior. Testing may include, for example, testing of the identification/authentication and audit mechanisms, penetration testing of key information system components, and testing security configuration settings. The assessor should be able to identify the various components in the information system, determine which security controls apply to the component, and prepare a strategy to adequately test each component.

Sample

Sampling is the process of selecting units (e.g., assessment objects) from a larger group or population of units so that, by studying the sample, one can generalize results back to the larger group or population from which the sampling was chosen. Since the scope and breadth of the examine, interview, and test skills require the skill of determining and using, for low-impact and moderate-impact systems, a "representative sample," and for high-impact systems, a "sufficiently large sample" of assessment objects, security assessment providers need to have experience in determining, analyzing, and reaching valid conclusions from such samples.

The assessment team should work together with the customer to select an appropriate sample size. The sample size should be large enough to provide the needed confidence that valid information will be obtained during the test, but not too large to incur unnecessary costs during the security assessment.

Penetration Testing

Penetration testing is a test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempts to circumvent the security features of an information system. Penetration testing can be used to enhance understanding of the information system, uncover weaknesses or deficiencies in the system, and to indicate the level of effort required to breach the system's security safeguards.

Although penetration testing is not required by SP 800-53A, assessors should be able to develop, conduct, and reach valid conclusions from penetration tests should the customer decide that such testing is warranted.

Other Skills

Assessment teams should demonstrate the following additional skills:

- Management skills (e.g., planning, scheduling, assigning tasks, reviewing, determining level of effort, and approving assessment results);
- Written and oral communication skills; and
- Interactions with technical and non-technical personnel (e.g., negotiating, sharing information, retrieving information).
- Skills can be demonstrated by describing projects in which the above skills were applied.

3.3.3 Assessment Team Ability Requirements

Security assessment teams should have the abilities (i.e., applications of knowledge to job functions) described below. Abilities are gained through experience.

Security Assessment Experience

Security assessors should have prior or current experience in providing security-related services to government agencies and departments or other organizations. Examples of such services include the following:

- Assisting in information system certifications or security control assessments;
- Reviewing required security documents or procedures for completeness and compliance with OMB and NIST requirements;
- Developing federally-required security documents, procedures, tests, or other products;

- Determining inherent and residual security risks;
- Determining whether, how, and to what extent federal legislation, NIST standards and guidelines, and OMB requirements pertain to a particular information system;
- Keeping up-to-date with current and new security threats, vulnerabilities, incidents, and solutions;
- Testing security controls;
- Designing security architectures or configurations;
- Operating information systems;
- Serving in security-related roles (e.g., information system security officer); and/or
- Providing advice regarding security.

Other Abilities and Experiences

Other abilities that the security assessors participating on an assessment team should possess include the following:

- **Analysis**—capability to sufficiently examine an activity, mechanism, or specification in accordance with the objectives of the analysis, draw conclusions, recognize incomplete or incorrect information, and recognize inconsistencies between or among assessment objects;
- **Problem-solving**—recognize and articulate problems, develop alternative solutions, select and justify a solution, and plan and implement a solution;
- **Understand the customer's missions and lines of business**—learn the background for communicating with the customer related to their goals and missions;
- **Interaction**—communicate with customers, management, and colleagues;
- **Test development**—determine tests that are appropriate to the assessment test objectives so that the assessment is efficient and cost effective;
- **Impact analysis**—determine the impacts of an assessment finding in order to present the information to the customer so they can assess the risk and determine the remediation priorities and strategy; and
- **Decision making**—analyze information and make appropriate decisions during the assessment.

Appendix A: References

1. FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

2. FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006.

3. *GAO Federal Information System Controls Audit Manual*, Version 1, May 2000.

4. ISO/IEC 17011, *Conformity Assessment—General Requirements for Accreditation Bodies Accrediting Conformity Assessment Bodies*, First Edition 2004-09-01.

5. ISO/IEC 17020, *General Criteria for the Operation of Various Types of Bodies Performing Inspection,* First Edition 1998-11-15.

6. ISO/IEC 1721;2006, *Conformity assessment -- Requirements for bodies providing audit and certification of management systems*

7. ISO/IEC 17024, *Conformity Assessment—General Requirements for Bodies Operating Certification of Persons*, First Edition 2003-04-01.

8. ISO/IEC 17025, *General Requirements for the Competence of Testing and Calibration Laboratories*, Second Edition 2005-05-15.

9. ISO/IEC 27006:2007, *Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems,* First Edition 2007-03-01

10. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4015, National Training Standards for System Certifiers, December 2000.

11. Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, June 2006.

12. NIST, *Managing Enterprise Risk in Today's World of Sophisticated Threats: A Framework for Developing Broad-Based, Cost-Effective Information Security Program*.

13. NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

14. NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

15. NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

16. NIST Special Publication 800-39, *Managing Enterprise Risk A Framework for Addressing Cyber Threats to Organizations, Individuals, and the Nation* (projected for publication October 2007).

17. NIST SP 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, December 2006.

18. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, Third Public Draft, June 2007.

19. NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

20. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Volumes 1 and 2, June 2004.

21. NIST SP 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004.

22. NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Process*, January 2005.

23. NIST SP 800-70, *Security Configuration Checklists Program for IT Products—Guidance for Checklists Users and Developers*, May 2005.

24. NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

Appendix B: Glossary

This appendix provides definitions for security terminology used within this NISTIR. The terms in the glossary are consistent with the terms used in the suite of FISMA-related security standards and guidelines developed by NIST. Unless otherwise stated, all terms used in this publication are also consistent with the definitions contained in the CNSS Instruction 4009, *National information Assurance Glossary*.

Ability [FISCAM]	The power to perform a job function while applying or using the essential knowledge
Accreditation [FIPS 200, NIST SP 800-37]	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Accreditation Boundary [NIST SP 800-37]	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.
Accrediting Authority	See Authorizing Official.
Activities	An assessment object that includes specific protection-related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic).
Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Assessment Procedure	One or more procedural steps that are created to achieve a set of assessment objectives by applying assessment methods to assessment objects.
Assessment Team	Two or more persons responsible for performing security control assessments in accordance with the assessment procedures in NIST Special Publication 800-53A. In some assessments an individual assessor may cover the responsibilities of the team.
Authorize Processing	See Accreditation.
Authorizing Official [FIPS 200, NIST SP 800-37]	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.

Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Certification [FIPS 200, NIST SP 800-37]	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Certification Agent [NIST SP 800-37]	The individual, group, or organization responsible for conducting a security certification.
Common Security Control [NIST SP 800-37]	Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.
Compensating Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.
Complete Assessment [NIST SP 800-53A]	An assessment in which all of the security controls in an information system are assessed. The certification and accreditation of a system requires a complete assessment.
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control [CNSS Inst. 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Customer	An individual or group of individuals that uses the services of a security assessment provider organization to conduct a security control assessment of a particular information system.
Examine	A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time.

Extended Assessment Procedure	A type of assessment procedure that is applied to an individual security control or a group of security controls (e.g., the set of security controls in a particular security control family or the set of security controls in an information system security plan) and works in conjunction with specialized assessment procedures in determining control effectiveness.
Federal Enterprise Architecture [FEA Program Management Office]	A business-based framework for government-wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
High-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.
Individuals	An assessment object that includes people applying specifications, mechanisms, or activities.
Information [FIPS 199]	An instance of an information type.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy [CNSS Inst. 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information System [44 U.S.C., Sec. 3502] [OMB Circular A-130, Appendix III]	A discrete set of information resources (e.g., personnel, equipment, funds, and information technology) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner (or Program Manager) [CNSS Inst. 4009, Adapted]	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Officer [CNSS Inst. 4009, Adapted]	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program.

Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Interview	A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time.
Knowledge [FISCAM]	The foundation upon which skills and abilities are built. Knowledge is an organized body of information, factors, principles, or procedures which, if applied, makes adequate performance of a job possible.
Low-Impact System [FIPS 200]	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.
Management Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Mechanisms	An assessment object that includes specific protection-related items (e.g., hardware, software, or firmware) employed within or at the boundary of an information system.
Moderate-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.

Non-repudiation [CNSS Inst. 4009]	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Operational Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
Organization [FIPS 200]	A federal agency or, as appropriate, any of its operational elements.
Partial assessment [NIST SP 800-53A]	An assessment in which a subset of the security controls in an information system is assessed. The continuous monitoring phase of the certification and accreditation process employs a partial assessment.
Penetration Testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Risk [FIPS 200, Adapted]	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment [NIST SP 800-30, Adapted]	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in-place security controls.

Risk Management [FIPS 200]	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
Sampling	The process of selecting units (e.g., assessment objects) from a larger group or population of units so that, by studying the sample, one can generalize results back to the larger group or population from which the sampling was chosen.
Security Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Security Assessment Plan	The plan that the assessment team develops and follows to determine the extent to which the security controls implemented in a particular information system are implemented correctly, operating as intended, and producing the desired outcomes with respect to meeting the security requirements for the system. Such a plan identifies the security controls to be assessed, the assessment procedures to be followed, the assessment objects to be examined or tested, and the customer personnel to be interviewed. The plan is provided to the customer for review and approval.
Security Assessment Provider Organization	A public or private sector organization responsible for conducting security assessments in accordance with NIST Special Publication 800-53A assessment procedures.
Security Assessment Report	The document that the assessment team develops to report the results of the security control assessment. The assessment team reports, for each assessment procedure performed, whether each determination statement in an assessment procedural step was "satisfied" or "other than satisfied." In the latter case, the assessment team indicates which parts of the security control were affected by the finding, describes how the control differs from the planned or expected state, and notes any potential compromises to confidentiality, integrity, and availability due to the "other than satisfied" result.
Security Category [FIPS 199]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

Security Controls [FIPS 199]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Control Baseline [FIPS 200]	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.
Security Requirements [FIPS 200]	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior Agency Information Security Officer [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.
Skill [FISCAM]	The proficient manual, verbal, or mental manipulation of people, ideas, or things. A skill is demonstrable and implies a degree of proficiency.
Specialized Assessment Procedure	A type of assessment procedure that is applied to an individual security control and works in conjunction with an extended assessment procedure in determining control effectiveness.
Specification	An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system.
System	See Information System.
System Security Plan [NIST SP 800-18, Rev 1]	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Tailoring	The process by which a security control baseline selected in accordance with the FIPS 199 security categorization of the information system is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls, where allowed.

Technical Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Test	A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time.
Threat [CNSS Inst. 4009, Adapted]	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Vulnerability [CNSS Inst. 4009, Adapted]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Appendix C: Acronyms

CNSS	Committee on National Security Systems
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standard
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act of 2002
GAO	Government Accountability Office
IEC	International Electrotechnical Commission
ISAP	Information Security Automation Program
ISO	International Organization for Standardization
ISSO	Information System Security Officer
IT	Information Technology
ITL	(NIST) Information Technology Laboratory
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OMB	Office of Management and Budget
POAM	Plan of Action and Milestones
SCAP	Security Content Automation Protocol
SDLC	System Development Life Cycle
SP	Special Publication
U.S.C.	United States Code

Appendix D: System Development Life Cycle[13]

In accordance with the provisions of FISMA, federal agencies are required to have an information security program and their security activities should be effectively integrated into the system development life cycle (SDLC). All information systems, including operational systems, systems under development, and systems undergoing some form of modification or upgrade, are in some phase of the SDLC. When fully implemented, the information system should be able to meet its requirements and do so in a manner that is secure enough to protect agency operations (including mission, functions, image, or reputation), agency assets, and individuals.

Security Integrated into Each System Development Life Cycle Phase

Customers of security assessment services should ensure that information security is addressed for each information system from concept to system disposal. Security should be integrated into each phase of the SDLC to ensure the system will be ready for the security assessment process. A traditional SDLC consists of five phase, each with its own security steps needed to effectively incorporate security into a system during its development:

- **Initiation Phase**— During the initiation phase, the need for a system is expressed and the purpose of the system is documented. Examples of security activities performed in this phase include security categorization, needs determination, and business impact assessment.
- **Acquisition and Development Phase**— During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. Examples of security activities performed during this phase include security requirements analysis, and security plan documentation.
- **Implementation Phase**— During this phase, the system will be installed and evaluated in the operational environment of the organization. Examples of security activities performed during this phase include certification and accreditation.
- **Operations/Maintenance Phase**— During this phase, the system is in place and functioning as intended. Enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced Examples of security activities performed during this phase include managing the configuration of the system, and continuously monitoring its security status.
- **Disposition Phase**— This phase provides for the disposal of the system in place. Examples of security activities performed during this phase include information preservation, media sanitization, and disposal of hardware and software.

NIST Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*, presents a framework for incorporating security into all phases of the SDLC process, from initiation to disposal.

Conducting Assessments During the System Development Life Cycle

Security assessments can be effectively carried out at various stages in the SDLC to increase the grounds for confidence or assurance that the security controls employed within the information system are effective. For example security assessments can be conducted by information system developers and by system integrators during the system development and acquisition phase of the

[13] NIST SP 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004.

life cycle to help ensure that the security control requirements for the protection of the system are properly designed, developed, and implemented.

Security assessments can also be conducted by the developers of commercial-off-the-shelf information technology component products that are to be used in organizational information systems. These types of assessments can be conducted either by the product developer during the development process or by independent, third-party testing laboratories during the implementation phase.

Security assessment can also be conducted by information system owners, security officers, independent certification agents, auditors, and inspectors general during the operations and maintenance phase of the life cycle to help ensure that the security controls are effective in the operational environment(s) in which the system is deployed. As part of the continuous monitoring phase, organizations select an appropriate subset of security controls to assess in a partial assessment. The subset should be based on the organization's assessment of risk, the plan of action and milestones, and organizational security policies, any of which may indicate the need for greater emphasis on selected security controls.

Finally at the end of the life cycle, security assessments can be conducted to ensure the important organizational information is purged from the information system prior to disposal.

Appendix E: NIST Risk Management Framework

The NIST Risk Management Framework[14] is an integral component of an organizational information security program. Security assessments are an important component of the Risk Management Framework – both in the original assessment of the security controls during the certification and accreditation process and in the ongoing monitoring of the controls. Figure E-1 illustrates the activities in the NIST Risk Management Framework, highlighting the specific activities related to security assessments, and denoting the information security standards and guidance documents associated with each activity.

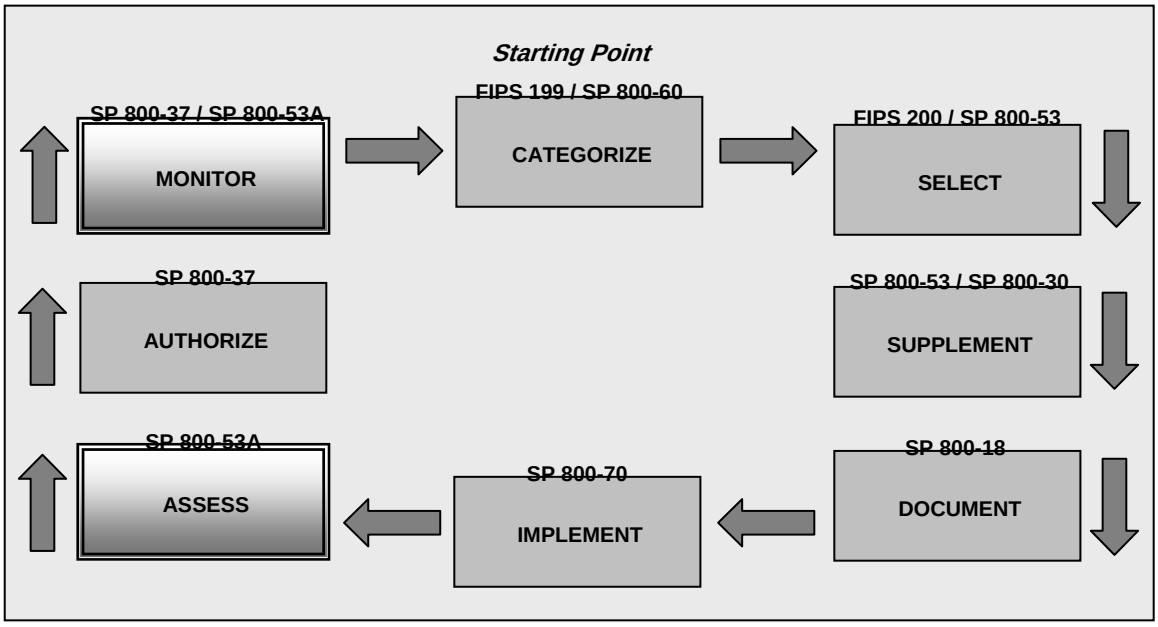

FIGURE E-1: THE RISK MANAGEMENT FRAMEWORK

The Risk Management Framework activities related to managing risk are paramount to an effective information security program and can be applied to both new and legacy information systems within the context of the SDLC and the Federal Enterprise Architecture. The activities include—

- ***Categorize*** the information system and the information resident within that system based on a FIPS 199 impact analysis.
- ***Select*** an initial set of security controls for the information system based on the FIPS 199 security categorization and the minimum security requirements defined in FIPS 200; apply tailoring guidance from NIST Special Publication 800-53, as appropriate, to obtain the control set used as the starting point for the assessing the risk associated with the use of the system.

[14] NIST Special Publication 800-39, *Managing Enterprise Risk A Framework for Addressing Cyber Threats to Organizations, Individuals, and the Nation* (projected for publication October 2007).

- ***Supplement*** the initial set of tailored security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.[15]
- ***Document*** the agreed-upon set of security controls in the system security plan including the organization's rationale for any refinements or adjustments to the initial set of controls.[16]
- ***Implement*** the security controls in the information system. For legacy systems, some or all of the security controls selected may already be in place.
- ***Assess*** the security controls using appropriate methods and procedures in accordance with NIST Special Publication 800-53A to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- ***Authorize*** information system operation based upon a determination of the risk to organizational operations and assets, to individuals, to other organizations, and to the nation resulting from the operation of the system and the decision that this risk is acceptable.[17]
- ***Monitor*** and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis.

[15] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, provides guidelines on the assessment and mitigation of risk.

[16] NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, provides guidance on documenting information system security controls.

[17] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidance on the security authorization of information systems.

Appendix F: Customer Readiness Review Checklist

The readiness review checklist should be used by customers to prepare for the security assessment and communicate the needed information about their organization to the security assessment team. The checklist is also used to validate that the customer has collected all relevant security documentation, identified appropriate individuals with knowledge of the information system and made them available for interviews, and will provide access to the information system.

Activity	Completed?	Comments
1. Obtain an independent security assessment team to assess any moderate- or high-impact information system.		
2. Establish the scope and objectives of the security assessment.		
3. Determine the level of effort and resources necessary to carry out the security assessment.		
4. Establish the time frame to complete the security assessment, including identifying the key milestone decision points.		
5. Notify key organizational officials of the impending security assessment.		
6. Validate that the system security plan is complete and includes all required information.		
7. Update the system security plan based on the independent analysis if the assessment is part of certification and accreditation.		
8. Select an appropriate set of security controls if the assessment is part of continuous monitoring activities, ensuring that all controls are assessed during a specified time period.		
9. Identify any administrative issues related to the assessment; communicate the information to the security assessment team and provide appropriate assistance.		
10. Make available the following documents or products to the security assessment team:		
10.1 Customer security policies and procedures		
10.2 Security materials associated with the implementation and operation of the security controls		
10.3 Information system		
10.4 Assurance products or other evidence developed during the acquisition/development or implementation phases of the		

Activity	Completed?	Comments
SDLC		
10.5 Assurance products or other evidence prepared during the assessment of common controls		
10.6 Assurance products or other evidence related to the implementation of service-oriented architecture		
11. Access to individuals that have knowledge about the implementation and operation of security controls. Depending on the specific assessment, individuals in the following roles may be interviewed:		
11.1 Information system owner		
11.2 Information system security officer		
11.3 System administrator		
11.4 Database administrator		
11.5 Web administrator		
11.6 Executives that are responsible for specific security functions		
11.7 Senior agency information security officer or CISO		
11.8 Authorizing official		
12. Approve the system security plan prior to initiating the security assessment.		

An effective enterprise-wide information security program provides a strong foundation for understanding and implementing security throughout the customer's organization. While the enterprise information security program is not within the information system owner's responsibilities or authority, the relevant security assessment activities conducted by the information security program should be considered and appropriate information shared with the assessment team.

Activity	Completed?	Comments
13. Apply NIST standards and guidelines to develop the information security program.		
14. Implement adequate information security policies and procedures consistent with NIST Special Publication 800-53.		

Activity	Completed?	Comments
15. Identify common security controls and assign responsibility for their independent assessment and share the results with information system owners.		
16. Integrate security into the SDLC and ensure security documentation is developed at the appropriate SDLC phase.		
17. Implement standard security assessment templates, tools, and techniques for assessment teams to follow.		
18. Procure automated tools to support the security assessment process as resources become available.		
19. Train security assessment teams on their organization-specific security assessment templates, tools, and techniques.		
20. Implement a continuous monitoring process.		
21. Implement and maintain a configuration/change management process to analyze the security impact of the requested change.		

Appendix G: Validation Checklist for Security Assessment Providers

The validation checklist can be used by both customers and the security assessment provider organizations. Using the checklist, customers can validate that the security assessment provider organization meets the requirements and demonstrates the capabilities required to effectively conduct and manage the security assessment process. The validation checklist can also be used by the security assessment provider organization to establish their security assessment practice and demonstrate their compliance with the requirements and expected capabilities.

Requirement	How Demonstrated	Validated?	Comments
1. Maintain independence from persons:			
1.1 Directly responsible for the development of the information system			
1.2 Responsible for day-to-day operation of the system			
1.3 Responsible for correcting security deficiencies			
2. Assign personnel separate from other security tasks to conduct security assessment services.			
3. Assign a technical manager to provide oversight to all security assessment tasks who is a permanent employee of the organization.			
4. Implement and maintain adequate administrative functions			
4.1 Contract services			
4.2 Time and attendance reporting			
4.3 Accounting and financial records			
4.4 Personnel			
4.5 Business records			

Requirement	How Demonstrated	Validated?	Comments
4.6 Training program			
5. Select personnel for each security assessment with the relevant knowledge, skills, and abilities related to the specific information system technologies and operating environment.			
6. Store securely and protect customer information related to the security assessment.			
7. Follow customer guidelines when transmitting security assessment information.			
8. Create and maintain standard procedures on how to complete the security assessment that are consistent with NIST standards and guidelines.			
9. Modify the organization's security assessment procedures to accommodate customer-specified tools, templates, and procedures.			
10. Report to the customer organization any discrepancies of customer's tools and templates relating to NIST standards and guidelines.			
11. Validate that the customer's readiness review is complete and that the customer has provided all information, documentation, and access needed to effectively conduct the assessment.			
12. Participate in an orientation meeting with the customer.			
13. Develop the security assessment plan with security assessment procedures and strategy that are appropriate to conduct the security assessment.			

Requirement	How Demonstrated	Validated?	Comments
14. Obtain the necessary approvals to execute the security assessment plan.			
15. Report any deficiencies in the system security plan to the customer for resolution.			
16. Conduct the security assessment following the security assessment plan and procedures.			
17. Identify each system component and develop a strategy to assess them.			
18. Select and use appropriate technical scanning and testing tools during the assessment.			
19. Document the results of the security assessment.			
20. Prepare the security assessment report, including recommendations for correcting deficiencies or eliminating vulnerabilities.			
21. Validate that the assessment team (collectively) has sufficient knowledge to conduct the security assessment.			
22. Validate that the assessment team (collectively) has the necessary skills to conduct the security assessment.			
23. Validate that the assessment team (collectively) has the required abilities (obtained through experience) to conduct the security assessment.			