NIST Special Publication 800-37

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems

Ron Ross and Marianne Swanson

C O M P U T E R 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

Version 1.0

October 2002

U.S. Department of Commerce

Donald L. Evans, Secretary

Technology Administration

Phillip J. Bond, Under Secretary of Commerce for Technology

National Institute of Standards and Technology

Arden L. Bement, Jr., Director

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's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems. This Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov — Phone: (202) 512-1800 — Fax: (202) 512-2250
Mail: Stop SSOP, Washington, DC 20402-0001

Authority

This document has been developed by NIST in furtherance of its statutory responsibilities under the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996 (specifically 15 United States Code (U.S.C.) 278 g-3 (a)(5)). This is not a guideline within the meaning of 15 U.S.C 278 g-3 (a)(3).

These guidelines are for use by Federal organizations which process sensitive information. They are consistent with the requirements of OMB Circular A-130, Appendix III.

This document may be used by non-governmental organizations on a voluntary basis. It is not subject to copyright.

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

National Institute of Standards and Technology Special Publication 800-37, 78 pages (October 2002) 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 BEGINS ON 28 OCTOBER 2002 AND ENDS ON 31 JANUARY 2003. COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, NIST, VIA ELECTRONIC MAIL AT SEC-CERT@NIST.GOV

OR VIA REGULAR MAIL AT

100 BUREAU DRIVE (MAIL STOP 8930)
GAITHERSBURG, MD 20899-8930

Acknowledgements

The authors, Ron Ross and Marianne Swanson of the National Institute of Standards and Technology (NIST) wish to thank their colleagues who reviewed drafts of this document and contributed to its development. In particular, we would like to acknowledge the contributions of Elaine Barker, Bill Burr, Tim Grance, Joan Hash, Arnold Johnson, Don Jones, Annabelle Lee, Mark Loepker, Terry Losonsky, Kean Miller, Brenda Moore, Karen Quigg, Ed Roback, George Rogers, Dennis Rosynek, Shannon Saia, Jack Sherwood, Ray Snouffer, Rodney Stalker, Gary Stoneburner, Carol Widmayer, and Bill Unkenholz, whose valuable insights improved the quality and usefulness of this document. We also gratefully acknowledge and appreciate the many comments we received from the federal certification and accreditation working group as well as readers in the public and private sectors.

Table of Contents

List of Figures

List of Tables

EXECUTIVE SUMMARY

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources* requires federal agencies to plan for security, ensure that appropriate officials are assigned security responsibility, and authorize system processing prior to operations and, periodically, thereafter. This authorization by senior agency officials is sometimes referred to as *accreditation*. The technical and non-technical evaluation of an IT system that produces the necessary information required by the authorizing official to make a credible, risk-based decision on whether to place the system into operation, is known as *certification*.

This special publication establishes a standard process, general tasks and specific subtasks to certify and accredit IT systems supporting the executive branch of the federal government. It provides a new approach to certification and accreditation (C&A) that uses the standardized process to verify the correctness and effectiveness of security controls employed in an IT system to ensure adequate security is maintained. The use of standardized, minimum security controls for low, moderate, and high levels of concern for confidentiality, integrity, and availability (defined in companion NIST Special Publication 800-53)[1] and the employment of standardized verification techniques and verification procedures (defined in companion NIST Special Publication 800-53A)[2] promote:

- More consistent, comparable, and repeatable certifications of IT systems;
- More complete, reliable information for authorizing officials—leading to a better understanding of complex IT systems and associated risks and vulnerabilities; and
- More informed decisions by management officials supporting the accreditation process.

While the certification and accreditation (C&A) process focuses on federal IT systems processing, storing, and transmitting sensitive (unclassified) information, the associated tasks and subtasks, security controls, and verification techniques and procedures, have been broadly defined so as to be universally applicable to all types of IT systems, including national security or intelligence systems, if so directed by appropriate authorities. As such, there may be occasional references within this publication to national security systems. These references are solely for the purpose of technical consistency and completeness in the development of a standardized C&A process for federal IT systems and should not be interpreted as providing guidance to agencies beyond the charter of NIST in fulfilling its statutory responsibilities under the Computer Security Act of 1987. State, local, and tribal governments as well as private sector organizations comprising the critical infrastructure of the United States are also encouraged to consider the use of the guidance provided in this special publication as appropriate. This special publication supersedes NIST Federal Information Processing Standards (FIPS) Publication 102, *Guidelines for Computer Security Certification and Accreditation*, September 1983.

1. Special Publication 800-53, *Minimum Security Controls for Federal Information Technology Systems*, is under development and will be made available by NIST for public comment by the Spring of 2003.

2. Special Publication 800-53A, *Techniques and Procedures for the Verification of Security Controls in Federal Information Technology Systems*, is under development and will be made available by NIST for public comment by the Spring of 2003.

CHAPTER ONE

1 INTRODUCTION

THE NEED FOR CERTIFICATION AND ACCREDITATION

Confidence in information technology security can be gained through actions taken during the processes of development, evaluation, and operation…

Information technology (IT) is the engine that drives our modern enterprises within the public and private sectors. Government agencies and businesses have become increasingly reliant on IT systems[3] to carry out important missions and functions and to increase enterprise productivity. These systems have become significantly more powerful during the past decade with an exponential growth in features and associated capabilities. The growth in features and capabilities has dramatically increased the complexity of the systems that comprise much of the critical information infrastructure within the United States. Complexity is a major concern when assessing the security of an IT system because the more complex a system is, the more difficult it is to thoroughly review all of its components. IT security includes operations that protect and defend information and systems by ensuring their confidentiality, integrity, and availability. This includes providing for the continual operations of systems by incorporating protection, detection and reaction capabilities. Ensuring that appropriate security objectives are developed and that the security risks are identified and balanced against operational demands is a fundamental management responsibility.

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources* requires federal agencies to plan for security, ensure that appropriate officials are assigned security responsibility, and authorize system processing prior to operations and, periodically, thereafter. These management responsibilities presume that responsible agency officials understand the risks and other factors that could adversely affect their mission goals. Moreover, these officials must understand the current status of security programs and controls in order to make informed judgments and investments that appropriately mitigate risk to an acceptable level. The goal of agency officials is both to operate their program and to do so with what OMB Circular A-130 defines as *adequate security*, or security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This definition explicitly emphasizes the risk-based policy for cost-effective security established by Public Law 100-235 (the Computer Security Act of 1987).

The authorization of an IT system to process, store, or transmit information, granted by a management official, provides a form of quality control and challenges managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. Some agencies refer to this authorization as *accreditation*. Accreditation, which is required under OMB Circular A-130, should be based on an assessment of the management, operational, and technical controls associated with an IT system. Since the security plan[4] prepared by an agency documents the protection requirements and security controls for an IT system, the

3. An IT system is a set of agency information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Categories of systems are *major applications* and *general support systems*, which include platform IT interconnections and outsourced IT processes. Chapter two provides a more detailed explanation of these categories of systems.

4. The completion of security plans for IT systems is a requirement of OMB Circular A-130 and the Computer Security Act of 1987. NIST Special Publication 800-18 provides guidance on recommended format and content of system security plans.

plan is the fundamental document required in the accreditation process, (thereby reducing unnecessary administrative duplication of effort), supplemented by more specific studies as needed.

In addition to the security plan, accreditation is also supported by a risk assessment and security evaluation. The risk assessment is described in the National Institute of Standards and Technology (NIST) Special Publication 800-30, *Risk Management Guide for Information Technology Systems*. The risk assessment identifies threats and vulnerabilities, analyzes security controls planned or in place, determines likelihood that specific vulnerabilities may be exploited, and provides an impact analysis. An initial risk assessment should be initiated on the IT system prior to beginning the accreditation process. The results of the initial risk assessment activities are used during the security evaluation and revisited and possibly revised based on the findings of the evaluation. The comprehensive evaluation of the technical and non-technical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements, is called *certification*. Certification provides the necessary information to a management official to formally declare that an IT system is approved to operate at an acceptable level of risk. The decision is based on the implementation of an agreed upon set of management, operational, and technical controls. By accrediting the system, the management official accepts the risk associated with it. Formalization of the accreditation process reduces the potential that systems will be operated without appropriate management review. Reaccreditation should occur prior to a significant change in the IT system, but at least every three years. It should be done more often where there is high risk and potential magnitude of harm.

1.1 Background

A significant percentage of federal IT systems in critical infrastructure areas have not completed needed security certifications, thus placing sensitive government information and programs at risk and potentially impacting national and economic security. Security certifications provide agency officials with the necessary information to authorize the secure operation of those IT systems. Currently, there are numerous competing security certification procedures within the federal government that are excessively complex, outdated, and costly to implement—resulting in assessments that are often inconsistent, flawed, and not repeatable with any degree of confidence. There is also a shortage of competent security expertise to conduct security certifications on the vast inventory of federal IT systems. To address these issues, NIST initiated a high priority project in March 2002 to accomplish the following tasks:

- Develop standard guidelines and procedures for certifying and accrediting federal IT systems including the critical infrastructure of the United States;
- Define essential minimum security controls for federal IT systems; and
- Promote the development of public and private sector assessment organizations and certification of individuals capable of providing cost effective, high quality, security certifications based on standard guidelines and procedures.

The specific benefits of the security certification and accreditation (C&A) initiative include:

- More consistent, comparable, and repeatable certifications of IT systems;
- More complete, reliable, information for authorizing officials—leading to better understanding of complex IT systems and associated risks and vulnerabilities—and therefore, more informed decisions by management officials;
- Greater availability of competent security evaluation and assessment services; and
- More secure IT systems within the federal government.

1.2 Purpose and Scope

The purpose of this special publication is to establish a standard process, general tasks and specific subtasks to certify and accredit IT systems supporting the executive branch of the federal government. While the C&A process focuses on federal systems processing, storing and transmitting sensitive (unclassified) information, the associated tasks and subtasks have been broadly defined so as to be universally applicable to all types of IT systems, including national security or intelligence systems, if so directed by appropriate authorities. As such, there may be occasional references within this publication to national security systems.[5] These references are solely for the purpose of technical consistency and completeness in the development of a standardized C&A process for federal IT systems and should not be interpreted as providing guidance to agencies beyond the charter of NIST in fulfilling its statutory responsibilities under the Computer Security Act of 1987. State, local, and tribal governments as well as private sector organizations comprising the critical infrastructure of the United States are also encouraged to consider the use of the guidance provided in this special publication as appropriate. This special publication supersedes NIST Federal Information Processing Standards (FIPS) Publication 102, *Guidelines for Computer Security Certification and Accreditation*, September 1983.

1.3 System Development Life Cycle

There are many types of federal IT systems requiring C&A—including legacy systems, new development systems, and systems undergoing some form of major or minor modification or upgrade. These systems can be characterized by describing where the system is in terms of the system development life cycle. Typically, there are five phases defined in the life cycle: (1) initiation, (2) development/acquisition, (3) implementation, (4) operations/maintenance, and (5) disposal. Elements of the standard C&A process defined in this special publication can be applied to any system during any phase of the life cycle. Most IT systems within the federal inventory of systems today are in a constant state of migration or evolution with new hardware, software and firmware being integrated on a routine basis. Rarely are completely new systems fielded all at once or taken out of the inventory all at once. Thus, the C&A process must be sufficiently flexible and dynamic to address the entire landscape of federal IT systems at any stage in the life cycle. For example, there is a significant difference in the type and level of system design documentation available for new development systems versus legacy systems, (i.e., legacy systems typically have considerably less information available). This simple difference can affect the degree and rigor of analyses and assessment activities that can be conducted during C&A. Accordingly, the C&A process, associated activities, tasks, and subtasks must reflect these potential differences and be designed to use whatever information is available to assist the authorizing official in making an informed risk-based decision to place the system into operation or authorize its continued operation.

1.4 Component Product Evaluation Programs

IT systems are procured and constructed to meet specific requirements and typically use existing commercial off-the-shelf (COTS) products such as operating systems, database systems, firewalls, network devices, web browsers, smart cards, biometrics devices, general purpose application components, and hardware platforms. The security countermeasures implemented by an IT system typically use functions of the underlying products and depend upon the correct operation

5. National security systems are those IT systems operated by the U.S. Government, its contractors, or agents that contain classified information or, as set forth in 10 U.S.C. Section 2315, that involve: intelligence activities or cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapon system, or equipment that is critical to the direct fulfillment of military or intelligence missions.

of those products and their security functions. The products may also be subject to a security evaluation themselves; such evaluations can support the C&A process. Standards such as the *Common Criteria for Information Technology Security Evaluation* (ISO/IEC Standard 15408) and the *Security Requirements for Cryptographic Modules* (FIPS 140-2) can be employed to obtain specific component product-level evaluations (sometimes called validations) in support of the C&A process.[6] A complete listing of validated, COTS products is provided by NIST at the following web sites: http://csrc.nist.gov/cryptval and http://niap.nist.gov/cc-scheme.

Using validated products can significantly reduce the cost of C&A by incorporating test and evaluation results or by providing information on how to securely configure a particular IT product within a system. Where a component product is incorporated or being considered for incorporation into multiple IT systems, there are also cost advantages to evaluating the security aspects of such a product independently and building a system from a catalogue of evaluated products. The results of such an evaluation should be expressed in a manner that supports the C&A process and the incorporation of the product into an IT system without unnecessary reevaluation. Guidance on how to securely configure COTS products can be instrumental in helping agencies develop, deploy, operate, and maintain more secure IT systems.

1.5 Relationship to Other NIST Security Publications

Special Publication 800-37 employs several NIST publications[7] in supporting the C&A process:

- Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998;
- Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, January 2002;
- Special Publication 800-53, *Minimum Security Controls for Federal Information Technology Systems*, (projected for Spring 2003); and
- Special Publication 800-53A, *Techniques and Procedures for the Verification of Security Controls in Federal Information Technology Systems*, (projected for Spring 2003).

Other NIST special publications provide additional guidance in a variety of security-related topic areas included in and supporting the C&A process:

- Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.
- Special Publication 800-14, *Generally Accepted Principles and Practices for Security Information Technology Systems*, September 1996;
- Special Publication 800-16, *IT Security Training Requirements: A Role-and Performance-Based Model*, April 1998;
- Special Publication 800-26, *Self-Assessment Guide for Information Technology Systems*, November 2001;

6. Notwithstanding the fact that evaluators can rely upon the prior validations of the individual components of the system (provided they are properly installed and configured), there must still be an evaluation of the integrated system to make certain that security holes have not been left in the integration process.

7. The security guidance documents listed in this chapter are recommended for use by all federal agencies. However, some agencies may employ different procedures and/or formats in developing security plans and in conducting risk management activities. The C&A process defined in this special publication allows for this potential diversity.

- Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2001;
- Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, December 2001;
- Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002; and
- Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, September 2002.

Figure 1.1 illustrates the relationship between NIST Special Publication 800-37 and other special publications supporting the C&A process. These publications can be obtained from the NIST Computer Security Resource Center (http://csrc.nist.gov).

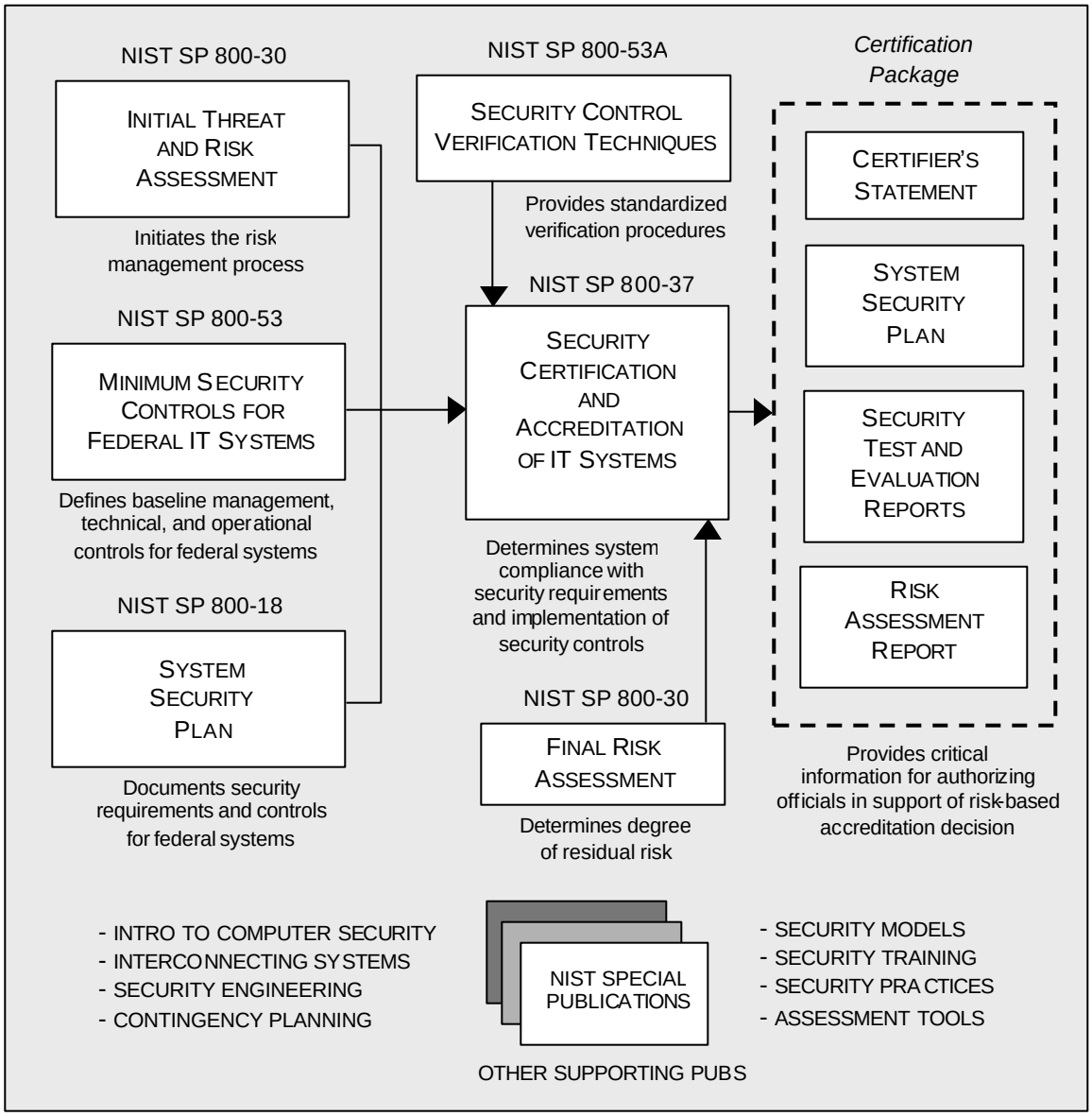

FIGURE 1.1 SPECIAL PUBLICATIONS SUPPORTING THE C&A PROCESS

1.6 Organization of this Special Publication

This special publication contains four main chapters and four supporting annexes. Chapter one introduces the fundamentals of C&A to include a statement of purpose and scope of applicability for the special publication. Chapter two describes the fundamental concepts associated with a C&A program to include the roles and responsibilities of key participants, types of IT systems subject to accreditation, accreditation categories, and types of accreditation decisions. Chapter three outlines the process for determining the appropriate Security Certification Level (SCL) and the relationship of certification levels to specified system security controls. Chapter four provides an overview of the different phases of the C&A process to include a brief description of the associated tasks within each phase. The supporting annexes provide more detailed C&A-related information to include references, glossary, acronym list, and sample accreditation letters.

CHAPTER TWO

2 THE FUNDAMENTALS

KEY PARTICIPANTS, TYPES OF SYSTEMS AND ACCREDITATION CATEGORIES

Outstanding agency security programs consider both technical and non-technical measures to build more secure systems, thus increasing the level of confidence individuals have in those systems…

This chapter focuses on the fundamentals of C&A including the roles and responsibilities of key participants in the C&A process, the types of IT systems that can be certified and accredited, and the various categories of accreditations that are available to federal agencies. The chapter also addresses the establishment of accreditation boundaries, the application of the C&A process to large and complex systems, and the types of accreditation decisions that can be rendered as well as the implications of those decisions on the security of the system and the agency.

2.1 Roles and Responsibilities

Throughout the life cycle of an IT system, many people have varying roles and responsibilities that impact the C&A process. The C&A approach described in this special publication allows agencies to adapt the specific C&A roles into their respective organizational structures to best manage the risks to the agency's mission. As discussed below, there are several important roles defined in a typical C&A program: (1) the authorizing official—often referred to as the *Designated Approving Authority (DAA)*, (2) the certifying official, (3) the program manager or system owner, and (4) the system security officer. Additional roles may be added to increase the integrity and objectivity of accreditation decisions in support of the system business case or mission. The actual titles may vary within an organization, but the responsibilities are the same. The number of participants in the C&A process and their assignments will differ between agencies based on the guidance set forth by the authorizing official, availability of resources, level-of-effort for certification, the security requirements, and the sensitivity and criticality of the system. The roles and responsibilities of the key participants in a C&A program are discussed below.

2.1.1 DESIGNATED APPROVING AUTHORITY

The DAA is a senior management official or executive with the authority to formally approve the operation of an IT system at an acceptable level of risk. Through accreditation, the DAA assumes responsibility for the risks of operation of the system in a specific environment. These officials have the authority to oversee and influence the budget and business operations of the systems under their jurisdiction. The DAA also approves security requirements documents, memorandums of agreement (MOA), memorandums of understanding (MOU), and any deviations from security policies. In addition to having the authority to approve systems for operation, the DAA has the authority to disapprove systems for operation and, if the systems are already operational, the authority to halt operations if unacceptable security risks exist.

Based on the information available in the final *certification package*, (i.e., security plan, developmental and/or operational ST&E reports, risk assessment report, and certifier's statement), the DAA can make a risk-based decision to: (1) grant system accreditation, (2) grant an interim approval to operate the system, or (3) deny system accreditation because the risks to the system are not at an acceptable level. The accreditation decision is documented in the final *accreditation package*, which consists of the accreditation letter and supporting documentation and rationale for the accreditation decision. In some situations, IT systems may involve multiple DAAs. If so,

agreements must be established among the responsible DAAs and the agreements should be documented in the accreditation package. In most cases, it is advantageous to agree to a lead DAA who represents the other DAAs during the C&A process.

2.1.2 CERTIFIER AND CERTIFICATION TEAM

The certification agent, or *certifier*, is the individual responsible for making a technical judgment of the IT system's compliance with stated security requirements, identifying, assessing, and documenting the risks associated with operating the system, coordinating the certification activities, and consolidating the final C&A packages. The certifier and certification team provide the expertise to conduct an independent technical and non-technical evaluation of a system based on the security requirements and security controls documented in the security plan. The certifier assesses the vulnerabilities in the system, determines if the security controls are correctly implemented and effective, and identifies the level of residual risk. To preserve the impartial and unbiased nature of the certification process, the certifier should be in a position that is independent from the persons directly responsible for system development and day-to-day operation. The certifier should also be independent of those individuals responsible for correcting security deficiencies identified during the certification process. Organizational independence of the certifier ensures the DAA receives the most objective information possible in order to make an informed, risk-based accreditation decision.

2.1.3 PROGRAM MANAGER AND SYSTEM OWNER

The *program manager* and *system owner* represent the interests of the user community and the IT system throughout the system's life cycle. The program manager is responsible for the system during initial development and acquisition and is concerned with cost, schedule, and performance issues. The system owner assumes responsibility for the system after delivery and installation during operation, maintenance, and disposal. The program manager and system owner ensure the system is deployed and operated according to the security requirements documented in the security plan and also ensure that system users and security support personnel receive the requisite security training (e.g., instruction in rules of behavior). The program manager and system owner coordinate the C&A effort and provide the necessary staff and information to the certifier and certification team when necessary. The program manager and system owner possibly fund the certification effort and can review the certification report prior to delivery to the DAA.

2.1.4 SYSTEM SECURITY OFFICER

For operational systems, the *system security officer* is responsible for the day-to-day security of a specific IT system including physical security, personnel security, incident handling, and security awareness, training, and education. The system security officer assists in the development of the system security policy and ensures compliance with that policy on a routine basis. The system security officer also identifies pending system or environment changes that may necessitate recertification and reaccreditation of the system. For developmental systems, the system security officer serves as the principal technical advisor to the program manager for all security-related issues.

2.1.5 OTHER SUPPORTING ROLES AND ROLE DELEGATION

There are other individuals within the agency such as the *user representative*, *security program manager*, *operations manager*, and *facility manager* that may also have concerns or interests in the C&A process. The user representative represents the operational interests of the user community and serves as the liaison for that community throughout the life cycle of the system. The user representative also assists in the C&A process, when needed, to ensure mission requirements are satisfied while meeting the security requirements defined in the security plan. The security pro-

gram manager ensures a standard C&A process is used throughout the agency, provides internal C&A guidance or policy, and, if appropriate, reviews certification packages prior to DAA review. The operations manager oversees the security operations and administration of the IT system to include performing backups, holding training classes, managing cryptographic keys, keeping up with user administration and access privileges, and updating security software. The facility manager oversees changes and additions to the facility housing the IT system and ensures changes in facility design or construction do not adversely affect the security of existing systems.

At the discretion of senior agency officials, certain C&A roles may be delegated. Agency officials may appoint appropriately qualified individuals, to include contractors, to perform the activities associated with a particular C&A role. The designated individuals are then able to operate with the authority of the agency officials within the limits defined for the specific activities. Agency officials retain ultimate responsibility, however, for the results of actions performed by these delegated individuals. The role and signature responsibility of the DAA should not be delegated to contractors. The DAA role has inherent United States Government authority, which should only be assigned to government personnel.[8] Figure 2.1 illustrates the roles and responsibilities of the key participants in the C&A process.

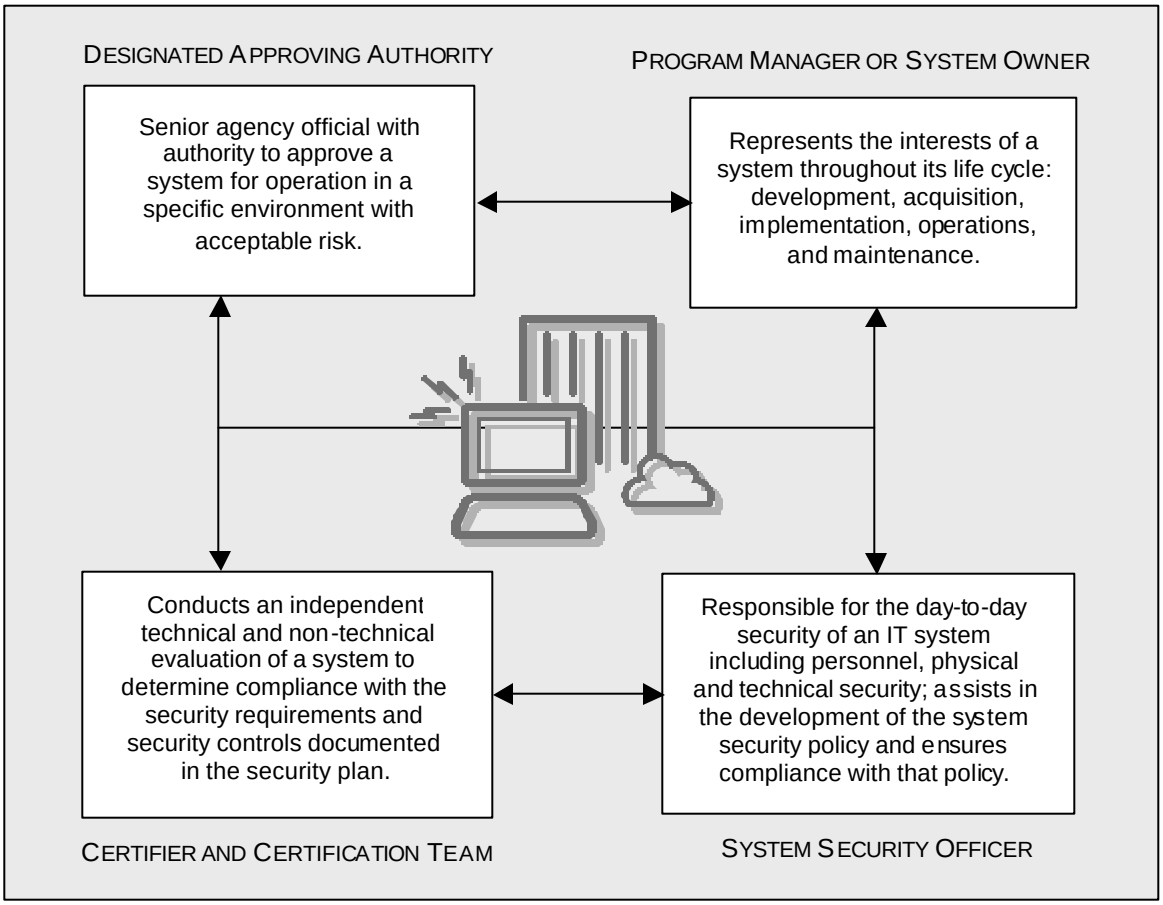

FIGURE 2.1 KEY PARTICIPANTS IN THE C&A PROCESS

8. Agencies should seek advice from the Office of the General Counsel prior to seeking exceptions to this practice and delegating authorization authority to non-governmental personnel.

2.2 The Landscape of IT Systems

In general, IT systems under the control of federal agencies fall into one of two categories: major applications or general support systems. OMB Circular A-130 requires all systems (major application and general support) to be authorized for processing. The C&A process can be applied to either type of system, as discussed below.

2.2.1 MAJOR APPLICATIONS

All federal applications have value and require some level of protection. Certain applications, because of the information processed, stored, or transmitted by the application, or because of the criticality of the application to the agency mission, require special management oversight. These applications are specified as *major applications*. Major applications are systems that perform clearly defined functions for which there are readily identifiable security considerations and needs, (e.g., an electronic funds transfer system or global command and control system). A major application might comprise many individual programs and hardware, software, and telecommunications components. These components can be a single software application or a combination of hardware/software focused on supporting a specific mission-related function. A major application may also consist of multiple individual applications if all are related to a single mission function (e.g., payroll or personnel).

2.2.2 GENERAL SUPPORT SYSTEMS

A *general support system* is a collection of interconnected information resources or computing environments under the same direct management control, which shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people, and provides support for a variety of users and/or common applications. A general support system, for example, can be a local area network (LAN) including smart terminals that support a branch office, a backbone network (e.g., agency-wide), communications network, departmental data processing center including its operating system and utilities, tactical radio network, office automation and electronic mail services, or shared information processing service organization. A general support system can also host one or more major applications. Agencies are expected to exercise management judgment in determining which of their applications are deemed major applications and to ensure that the security requirements of non-major applications are discussed as part of the security considerations for the applicable general support systems.

2.2.3 PLATFORM IT INTERCONNECTIONS AND OUTSOURCED IT PROCESSES

Two special cases of either a major application or general support system should also be considered when identifying systems for C&A: (1) platform IT interconnections, and (2) outsourced IT-based processes. Platform IT interconnection refers to network access to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons systems, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, and utility distribution systems (for example, water and electric distribution systems). An outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector IT systems, outsourced information technologies, or outsourced information services. Both platform IT interconnections and outsourced IT-based processes have readily identifiable security considerations and needs that must be addressed during the C&A process. Typically, the C&A process defined in this special publication can be easily adapted for these special cases.

2.3 Accreditation Categories

There are three types of accreditations that can be obtained by federal agencies: (1) system accreditation, (2) type accreditation, and (3) site accreditation. The accreditation category is an important concept that plays a central role in the subsequent tasks and subtasks undertaken during the C&A process. The accreditation category describes how the IT system will be viewed during C&A—that is, as a one-of-a-kind major application or general support system, as a more generic type of application or system that will be replicated in many different locations, or as a group of applications and/or systems under a common DAA at a specific, self-contained location or proximate geographic area. Each accreditation category addresses a different accreditation need and is closely related to the certification process associated with it. Authorizing officials should choose the type of accreditation best suited to the agency's needs. The accreditation categories are explained in greater detail below.

2.3.1 SYSTEM ACCREDITATIONS

A *system accreditation* is the most common type of accreditation that authorizes the operation of a major application or a general support system at a particular location with specified environmental constraints. A system accreditation for a major application or a general support system is warranted when information resources require special security considerations because of the risk and magnitude of the harm resulting from the loss, misuse or unauthorized access to or modification of the information or information resources involved. The certification process will assess all of the relevant security controls, (i.e., management, operational, and technical controls) for the major application or general support system with the resulting accreditation authorizing operation at an agreed upon level of residual risk. Figure 2.2 illustrates the concept of system accreditation.

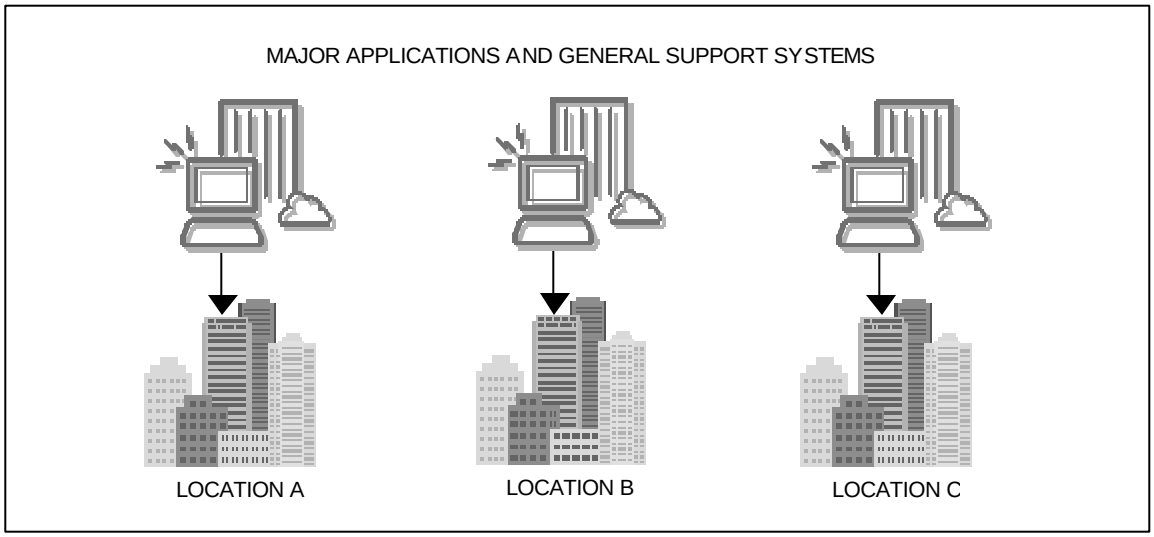

FIGURE 2.2 SYSTEM ACCREDITATIONS

2.3.2 TYPE ACCREDITATIONS

In some situations, a major application or general support system is intended for installation at multiple locations. The application or system usually consists of a common set of hardware, software, and firmware. Since it is difficult to accredit a common application or system at all possible locations, the DAA may issue a *type accreditation* for typical operating environments. Type accreditations are a form of interim accreditation (See Section 2.6.2) and are used to certify and accredit multiple instances of a major application or general support system for operation at ap-

proved locations with the same type of computing environment. The DAA must include a statement of residual risk and clearly define the intended operating environment for the major application or general support system. The DAA must also identify specific uses of the application or system and operational constraints and procedures under which the application or system may operate. Type accreditations provide an efficient way to accredit major applications and general support systems meeting specified security requirements and employing selected security controls for a single application or system distributed to multiple locations. Type accreditations tend to significantly reduce the field-level assessment activities because the local organization is provided with the initial system documentation needed for accreditation, including specific security operating procedures.

To support type accreditations of major applications and general support systems, initial security testing and evaluation, sometimes referred to as developmental Security Test and Evaluation (ST&E), should occur at a central integration and test facility or at one of the intended operating sites, if a test facility is not available. Software and hardware security testing of common system components at multiple sites is not recommended. At the conclusion of the developmental ST&E, the system security plan, the developmental ST&E report, and the initial risk assessment report are collected in the final developmental certification package and forwarded along with the certifier's statement to the DAA[9]. The accreditation package containing the security plan and any documentation supporting the final accreditation decision is then sent with the software and hardware suite to each site where the major application or general support system will be installed. The site will not need to repeat the baseline ST&E conducted during the type accreditation. However, the system installation and security configuration should be tested at each operational location during operational (or site) ST&E. With type accreditations, local personnel at the installation site assume responsibility for monitoring the operational environment for compliance with the stated assumptions about the environment and approved configurations as described in the accreditation documentation. Figure 2.3 illustrates the concept of type accreditation.

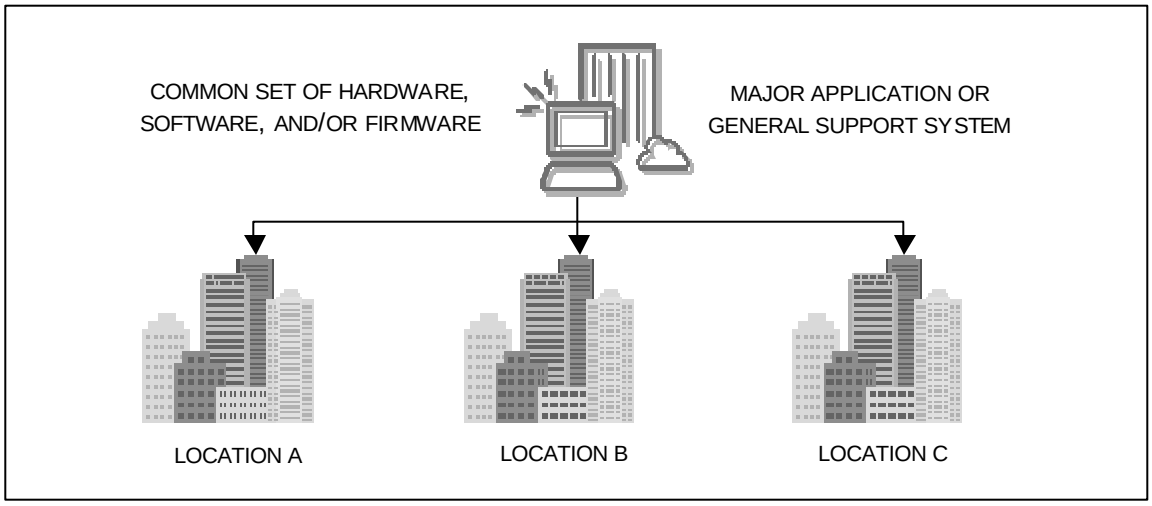

FIGURE 2.3 TYPE ACCREDITATIONS

9. During new system development and acquisition, the authorizing official rendering type accreditation decisions is sometimes referred to as the *developmental DAA*. The developmental DAA identifies and accepts the risk for the design of the new system and is also responsible for understanding the typical operational environments where the system will be deployed and the security requirements that the system will be required to satisfy. The type accreditation and supporting documentation is used by the *operational DAA*, who then takes the fielded system and initiates a local accreditation, accepting responsibility for the system configuration, operating environment, and operational risks.

2.3.3 SITE ACCREDITATIONS

If several agency organizations are in a self-contained location within a proximate geographic area, serve under a common senior executive, face common threats, share a common mission, and have comparable vulnerabilities, then the DAA may issue a *site accreditation* applicable to all major applications and/or general support systems on the site. Site accreditations focus on obtaining accreditation of an entire facility and the suite of applications and systems resident therein. Figure 2.4 illustrates the concept of site accreditation.

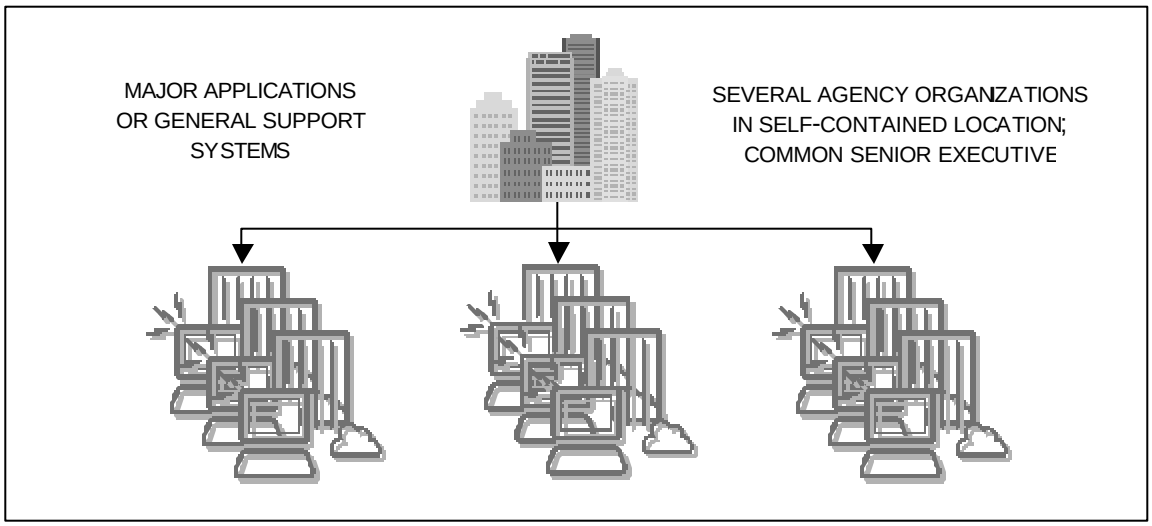

FIGURE 2.4 SITE ACCREDITATIONS

2.4 Certification and Accreditation Documentation

It is important to remember that the purpose of the C&A process is to provide the DAA with the information necessary to make an informed, risk-based decision regarding the operation of an IT system in a specific environment. As such, each task and subtask in the C&A process is carefully crafted to support the ST&E activities needed to determine compliance with system security requirements and if the selected security controls identified in the security plan are correctly implemented and effective. The *certification package* is the final set of documentation produced by the certifier and the certification team for the DAA. The certification package normally consists of: (1) the security plan (revised and updated as necessary), (2) the developmental and/or operational ST&E reports, (3) the final risk assessment report, and (4) the certifier's statement. Each of these documents is described briefly below.

2.4.1 SYSTEM SECURITY PLAN

The system security plan plays a central role in the risk management and C&A processes and in documenting the security posture of an agency's IT system. The purpose of the security plan is to provide an overview of the security requirements for the IT system and to describe the existing or planned security controls (management, operational, and technical) for meeting those requirements. The security plan also provides a full description of the system and delineates responsibilities and expected behavior of individuals who access the system. Agencies that have completed their security plans prior to the start of the C&A process can effectively use the information contained in those plans to support the initial pre-certification activities. Agencies that have not completed their security plans can generate the needed information for the plans by conducting the initial pre-certification activities required by the C&A process. It should be noted that the security plan is a living document that is updated throughout the system development life cycle as new

information becomes available. If the security plan was written prior to the system undergoing a risk assessment, the security plan should be updated with the risk assessment results. The security plan should contain, at a minimum, the information outlined in NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998. Additional information may be included at the discretion of the DAA in accordance with agency policies or directives.

2.4.2 SECURITY TEST AND EVALUATION REPORTS

ST&E activities are an essential component of the C&A process. The purpose of ST&E is to determine the IT system's compliance with the security requirements documented in the security plan and to verify that the security controls identified in the plan are correctly implemented and effective. There are two distinct types of ST&E that can be employed during the C&A process: (1) developmental ST&E and (2) operational ST&E. Developmental ST&E is conducted on new systems (or systems undergoing major upgrades) during the development and acquisition phase of the system development life cycle. Operational ST&E is conducted on new or upgraded systems (after delivery and installation) during the implementation phase of the life cycle or on legacy systems during the operation/maintenance phase of the life cycle. Developmental ST&E reports typically contain the results of testing and evaluation conducted on the system's hardware, software, and firmware (including architectural design analyses and functional testing) to verify that the technical security controls are implemented correctly and are effective in satisfying the security requirements levied on the system. Developmental ST&E relies more heavily on the detailed system design documentation that is usually only available for new systems.[10] Operational ST&E reports typically contain the results of testing and evaluation conducted on the IT system at the site where the system is deployed for operation to verify that the technical, management, and operational security controls are implemented correctly and are effective in satisfying the system security requirements. Operational ST&E may include functional testing, penetration testing, and vulnerability analyses. For new systems (and major system upgrades) undergoing C&A, there will be both a developmental ST&E report and an operational ST&E report. For legacy systems (or systems with minor modifications) undergoing C&A, there will only be an operational ST&E report.

2.4.3 RISK ASSESSMENT REPORT

The risk assessment determines the degree of risk associated with the confidentiality, integrity, and availability of the IT system and the information it processes, stores, and transmits. The risk assessment report documents the results of the risk assessment activities and includes the threats to and the vulnerabilities of the system, proposals for and evaluations of the effectiveness of various security controls, the trade-offs associated with the controls (e.g., performance impact and cost), and the residual risk associated with a candidate set of controls. For each residual risk, the report specifies the rationale for accepting or rejecting the risk and possible future security controls to mitigate the risk. The certifier evaluates the final risk assessment report, carefully judging the scope and accuracy of its findings. The certifier's statement to the DAA is based on the information contained in the risk assessment report and other supporting documents. The DAA uses the risk assessment report along with the other documents provided in the certification package to make the final accreditation decision. The risk assessment report should contain, at a minimum, the information outlined in NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, October 2001. The security plan for the system should be modified to include the findings and planned actions resulting from the risk assessment. Additional infor-

10. Developmental ST&E reports are also produced for systems that are being type accredited as an interim step prior to final accreditation at the operational site.

mation may be included at the discretion of the certifier or DAA in accordance with agency policies or directives.

2.4.4 CERTIFIER'S STATEMENT

The certifier's statement provides an overview of the security status of the system and brings together, all of the information necessary for the DAA to make an informed, risk-based decision. The statement documents that the security controls are correctly implemented and effective in their application. The report also documents the security controls not implemented and provides corrective actions.

2.5 Accreditation of Large and Complex Systems

Establishing an appropriate accreditation boundary for the C&A process has always been one of the most challenging problems for an agency. Boundaries that are too expansive make the C&A process unwieldy and far too difficult for most agencies to handle. Boundaries that are too limited increase the number of C&A processes that must be completed and thus, drive up the total cost for the agency. In addition to the accreditation boundary dilemma, the increasing presence of large and complex systems (both major applications and general support systems) is also exacerbating the certification aspect of the C&A process. The application of selected security controls (management, operational, and technical) across a large and complex system may be cost prohibitive and technically infeasible. Accordingly, any attempt to certify such a system to a single certification level[11], (i.e., applying the same level of rigor with regard to testing, evaluation, and systems analysis), to determine compliance with the system security requirements and if the security controls are correctly implemented and effective, may also be unrealistic.

To solve this problem, DAAs should consider the nature of the IT system being considered for C&A and the feasibility of decomposing the system into more manageable components. The decomposition of large and complex systems into system-level components, or *subsystems*, facilitates the application of the certification process in a more cost effective manner and supports the concepts of risk management and defense-in-depth. A defense-in-depth strategy recognizes that an IT system can be viewed as a wide-ranging interconnected, end-to-end set of information capabilities managed as a single enterprise. Thus, for both major applications and general support systems, the DAA may define a set of subsystem components in the security plan. Each subsystem component is fully characterized in the plan and an appropriate set of security requirements and security controls identified for that component.

When the certification process begins, each subsystem component may be certified at a different certification level, depending on the levels of concern[12] expressed by the agency for confidentiality, integrity, and availability of that component within the system. The critical, high value, subsystem components, as identified by increasing levels of concern for confidentiality, integrity, or availability, demand and receive more rigorous and intensive analyses during the certification process than the less important, low-value subsystem components. The final system accreditation may contain one or more subsystem components certified to the appropriate level based on the documented levels of concern and associated security controls. The certification package is modified to include multiple ST&E reports (one for each subsystem component) together with a final

11. Certification levels are described in greater detail in Chapter 3 of this special publication.

12. During the pre-certification phase of the C&A process, agencies validate the levels of concern identified in the security plan for the confidentiality, integrity, and availability of their IT systems and the information processed, stored and transmitted by those systems. The levels of concern, in turn, influence the selection of appropriate security controls for the system and the ultimate certification level required. These concepts are described in Chapter 3 of this special publication.

risk assessment report that reflects the total risk to the system as a whole. The total risk to the IT system may be greater than the sum of the risks to the individual subsystem components.

To illustrate a simple example of system decomposition, a general support system contains a guard that monitors the flow of information between two LANs, where the information contained in one of the networks is at a different sensitivity level than the other network. The system, in this case, can be partitioned into three subsystem components: (1) LAN Alpha, (2) LAN Bravo, and (3) the guard separating the two LANs. The guard subsystem component must be highly trusted to do its assigned security tasks, (i.e., only letting certain information pass between the respective LANs). The security requirements and associated security controls levied on this particular subsystem component might be quite extensive since there is obviously a high level of concern for the confidentiality of the information in the system. The guard subsystem component will be certified at a higher level than the other two LAN subsystem components. The rigor of the certification process at the higher certification levels reflects the need for greater assurance for the guard versus the other components in the system. Additional testing, evaluation, and analysis is required for each successive certification level. Isolating the high-value subsystem components in a system and applying the appropriate certification level to those components is a cost-effective method of accrediting an IT system. Figure 2.5 illustrates the concept of subsystem component certification and the associated accreditation for a large and complex agency system.

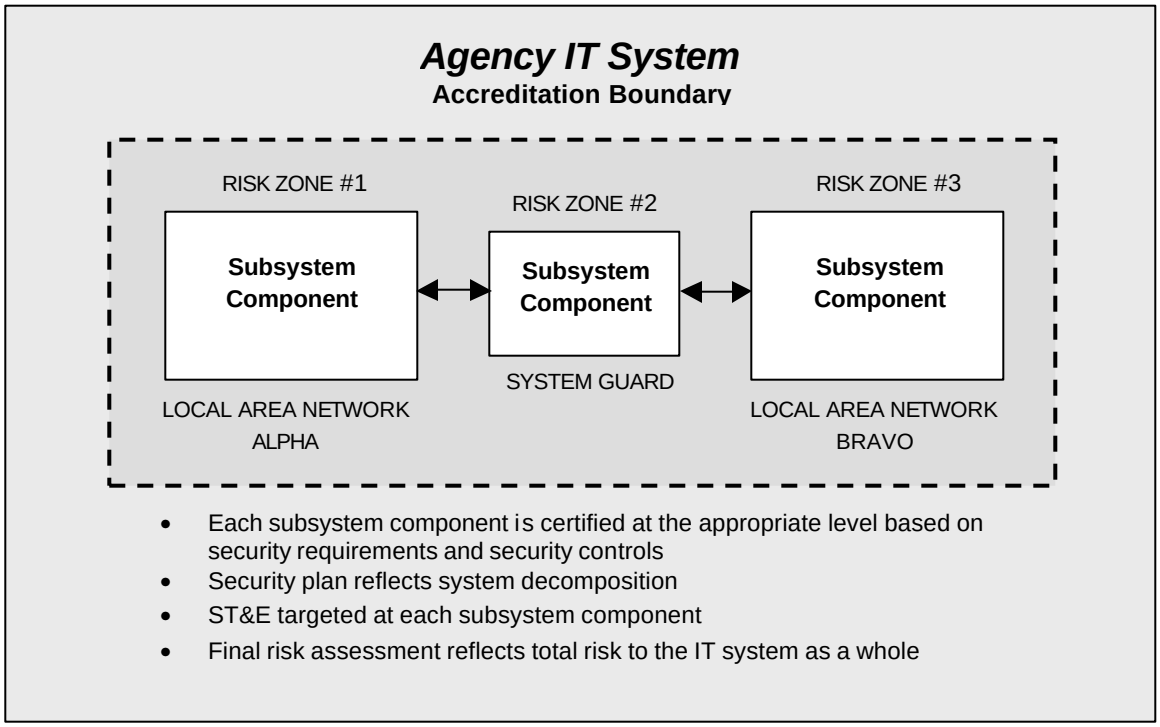

FIGURE 2.5 SYSTEM DECOMPOSITION EXAMPLE

2.6 Accreditation Decisions and Residual Risk

After the completion of system certification, the DAA is presented with the key information contained in the certification package, (i.e., the final system security plan, the ST&E report(s), the final risk assessment report, and the certifier's statement). The certification process has determined and documented which security controls have been implemented correctly and are operating effectively in satisfying the IT system security requirements. Any remaining vulnerabilities in

the IT system after employment of the designated security controls, forms the basis of the residual risk for the system. It is with this documented information that the DAA considers the remaining risk to the system and decides whether or not to authorize processing, placing the system into operation and accepting the residual risk. Based on the given situation, the DAA will choose one of the following accreditation options when rendering a final accreditation decision: (1) *full accreditation*, (2) *interim accreditation*, or (3) *accreditation disapproval.*

2.6.1 FULL ACCREDITATION

In the case of full accreditation, the system security requirements have been satisfied and the security controls have been implemented correctly and are operating effectively. The system is approved to operate in the intended environment as stated in the security plan and few, if any, restrictions on processing apply. The DAA issues an appropriate accreditation letter along with any supporting documentation justifying the accreditation decision. This information is part of the final *accreditation package.* System accreditation decisions by the DAA are conveyed in the final accreditation package. The accreditation package normally consists of the following: (1) the accreditation letter, (2) the security plan, and (3) a report documenting the basis for the accreditation decision. In most cases, the DAA's report can be constructed from information provided in the certification package. Certain information from the security plan, ST&E reports, and risk assessment report may, at the discretion of the DAA, be withheld in the final accreditation package due to its sensitive nature.

2.6.2 INTERIM ACCREDITATION

For interim accreditation, the system does not currently meet the security requirements as stated in the security plan and all of the necessary security controls are not implemented and operating effectively. However, mission criticality mandates the system become operational and no other capability exists to adequately perform the mission.[13] The interim accreditation, or initial approval to operate, is a temporary approval that may be issued for a limited period of time as specified by the DAA. If the DAA is inclined to approve an interim accreditation, the operational restrictions imposed to mitigate the increased risk should be carefully reviewed, and an interim accreditation action plan should be developed that acknowledges the following:

- Mission criticality necessitates immediate operation of the system;
- Interim accreditation is in the best interest of the organization;
- Resources are available to complete the action plan and the needed certification tasks;
- The action plan can be completed within the allowable time specified by the DAA; and
- Operational restrictions lessen the risk to the lowest level possible (at this time) and the residual risk is acceptable.

The DAA issues an appropriate interim accreditation letter conveying the above conditions and restrictions and providing supporting documentation, as necessary.

Type accreditations are considered a form of interim accreditation since the operational ST&E on the system has not yet been conducted to verify that the site-related security requirements have been satisfied and that the site-related security controls are correctly implemented and effective. Once the accreditation is granted, the DAA at the operational site accepts responsibility for the security of the system and for the information it processes, stores, and transmits.

13. This type of interim accreditation may be necessary for many legacy systems that cannot meet existing security requirements, but must be operational until a replacement system (or major system upgrade) is acquired.

2.6.3 ACCREDITATION DISAPPROVAL

In the case of accreditation disapproval, the system does not meet the security requirements and security controls as stated in the security plan; residual risk is too great, and mission criticality does not mandate the immediate operational need. Therefore, the developmental system is not approved for operation or, if the system is already operational, the operation of the system is halted. The DAA issues the appropriate accreditation disapproval letter including any supporting documentation justifying the accreditation disapproval decision.

CHAPTER THREE

3 SECURITY CONTROLS AND CERTIFICATION LEVELS

TAILORING THE PROCESS TO AGENCY NEEDS

Knowing the value of your information assets and the legitimate, realistic threats to those assets is critical to determining the level of security needed by the agency, and thus the amount of resources that should reasonably be applied to achieving that security…

This chapter describes the process for selecting the necessary security controls required to adequately safeguard the IT system and for determining the appropriate certification level for the system. To support that process, it is important to understand the fundamental characteristics of an IT system with regard to security. These characteristics, expressed in the concepts of system criticality/sensitivity and system exposure to internal and external threats, affect the ultimate selection of security controls and the certification level. The introductory section of this chapter explains how to characterize an IT system and the subsequent sections describe how the system characterization affects the selection of security controls and the certification level. The selection of security controls and certification level for the IT system can be accomplished independently of one another based on the agency's expressed levels of concern for confidentiality, integrity, availability, and system exposure. Specific security controls for IT systems can be found in a companion NIST Special Publication 800-53, *Minimum Security Controls for Federal Information Technology Systems*, (projected for Spring 2003).

3.1 Characterizing Information Technology Systems

It is important to accurately characterize an IT system in order to set the stage for the eventual selection of appropriate security controls—controls which are ultimately responsible for safeguarding the system and for satisfying the agency's security requirements. Characterizing an IT system can be accomplished by: (1) examining the *criticality/sensitivity* of the system and the information the system processes, stores, and transmits, (2) assessing the *exposure* of the system and its information to both internal and external threats, and (3) assigning appropriate *levels of concern* for both system sensitivity and exposure. Each of these topics is described in greater detail below.

3.1.1 SYSTEM CRITICALITY/SENSITIVITY

System criticality/sensitivity is a measure of the importance and nature of the information processed, stored, and transmitted by the IT system to the organization's mission and day-to-day operations. The criticality/sensitivity of an IT system and its information can be addressed by analyzing the system requirements for confidentiality, integrity, and availability. System *confidentiality* provides assurance that the information in an IT system is protected from disclosure to unauthorized persons, processes, or devices. System *integrity* provides assurance that information in an IT system is protected from unauthorized, unanticipated, or unintentional modification or destruction. System integrity also addresses the quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. System *availability* provides assurance that information, services, and IT system resources are accessible to authorized users and/or system-related processes on a timely and reliable basis and are protected from denial of service. By performing this analysis, the value of the system can be determined. The value is one of the major factors in risk management.

3.1.2 SYSTEM EXPOSURE

System exposure is a measure of the potential risk to an IT system from both external and internal threats. *External system exposure* relates to the method by which users access the system, (e.g., dedicated connection, intranet connection, Internet connection, wireless network), the existence of backend connections to the system and to what the backend systems are connected, and the number of users that access the system. *Internal system exposure* relates to the types of individuals that have authorization to access the system and the information the system stores, processes, and transmits. It includes such items as individual security background assurances and/or clearance levels, access approvals, and need-to-know. Internal system exposure is considered for IT systems that are processing, storing, or transmitting (classified) national security information or (unclassified) sensitive information with high confidentiality requirements. It is also considered for IT systems with high integrity requirements. The concept of system exposure and how it relates to confidentiality, integrity, and availability in the C&A process, will be discussed later in this chapter.

3.1.3 LEVELS OF CONCERN

Confidentiality, integrity and availability are important security factors that should be considered when assessing the overall security of an IT system. These security factors are described in section 3534(a)(1)(A) of the Government Information Security Reform provisions of the National Defense Authorization Act of 2000. The level of concern for confidentiality is based on the tolerance for unauthorized disclosure or compromise of information on the system.[14] The level of concern for integrity is based on the tolerance for unauthorized modification or destruction of information on the system. The level of concern for availability is based on the tolerance for delay in the processing, transmission, or storage of information on the system or the tolerance for the disruption or denial of a service provided by the system.

As described in NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, when determining appropriate levels of concern, agencies need to consider any laws, regulations, directives, instructions, or policies that establish specific requirements for confidentiality, integrity, or availability of data or information on the system. Examples might include Presidential Decision Directive 63, the Privacy Act of 1974, the Computer Security Act of 1987, the Healthcare Information Portability and Accountability Act of 1996, trade secret laws, patent and copyright laws, federal acquisition regulations, the code of federal regulations, or a specific statute or regulation concerning agency data or information, (e.g., tax or census information). Mission requirements also need to be considered. An assessment should be performed

14. Information within federal systems, unless otherwise specified, typically falls into one of two categories: (1) *sensitive information* (unclassified), and (2) *national security information* (classified). Sensitive information includes any information the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (The Privacy Act of 1974), but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Some specific categories of sensitive information are protected by statute, regulation or contract, (e.g., privacy information, proprietary information, export control information, pre-publication academic information). National security information includes any information that has been determined pursuant to Executive Order 12958 or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. National security information includes Sensitive Compartmented Information (SCI) concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

by the agency to determine the levels of concern for the system based on the identified requirements for confidentiality, integrity, and availability. A value of low, moderate, or high is then assigned to each factor. Table 3.1 provides guidance to agencies in assigning values to the levels of concern for confidentiality, integrity and availability.

TABLE 3.1 LEVELS OF CONCERN FOR SYSTEM CRITICALITY/SENSITIVITY

	LOW	MODERATE	HIGH
CONFIDENTIALITY SENSITIVE INFORMATION (UNCLASSIFIED)	The consequences of unauthorized disclosure or compromise of data or information in the system are **generally acceptable**. Loss of confidentiality could be expected to affect agency-level interests and have some negative impact on mission accomplishment.	The consequences of unauthorized disclosure or compromise of data or information in the system are only **marginally acceptable**. Loss of confidentiality could be expected to adversely affect agency-level interests, degrade mission accomplishment or create unsafe conditions that may result in injury or serious damage.	The consequences of unauthorized disclosure or compromise of data or information in the system are **unacceptable**. Loss of confidentiality could be expected to adversely affect national-level interests, prevent mission accomplishment or create unsafe conditions that may result in loss of life or other exceptionally grave damage.
CONFIDENTIALITY NATIONAL SECURITY INFORMATION (CLASSIFIED)	Not applicable.	Not applicable.	The consequences of unauthorized disclosure or compromise of data or information in the system are **unacceptable**. Loss of confidentiality could be expected to cause exceptionally grave damage, serious damage, or damage to the national security.
INTEGRITY	The consequences of corruption or unauthorized modification of data or information in the system are **generally acceptable**. Loss of integrity could be expected to affect agency-level interests and have some negative impact on mission accomplishment.	The consequences of corruption or unauthorized modification of data or information in the system are only **marginally acceptable**. Loss of integrity could be expected to adversely affect agency-level interests, degrade mission accomplishment or create unsafe conditions that may result in injury or serious damage.	The consequences of corruption or unauthorized modification of data or information in the system are **unacceptable**. Loss of integrity could be expected to adversely affect national-level interests, prevent mission accomplishment or create unsafe conditions that may result in loss of life or other exceptionally grave damage.
AVAILABILITY	The consequences of loss or disruption of access to system resources or to data or information in the system are **generally acceptable**. Loss of availability could be expected to affect agency-level interests and have some negative impact on mission accomplishment.	The consequences of loss or disruption of access to system resources or to data or information in the system are only **marginally acceptable**. Loss of availability could be expected to adversely affect agency-level interests, degrade mission accomplishment or create unsafe conditions that may result in injury or serious damage.	The consequences of loss or disruption of access to system resources or to data or information in the system are **unacceptable**. Loss of availability could be expected to adversely affect national-level interests, prevent mission accomplishment or create unsafe conditions that may result in loss of life or other exceptionally grave damage.

3.1.3.1 External System Exposure

In addition to determining levels of concern for confidentiality, integrity, and availability, consideration should also be given to determining levels of concern for internal and external system exposure. Consider the potential exposure of the IT system to external threats by using the following external exposure factors: (1) access method, (2) backend connections, and (3) number of authorized users. Assign a level of concern value, (i.e., low, moderate, or high), to each of the designated external exposure factors. The level of concern for external system exposure is the highest value of the values assigned to each of the individual exposure factors. For example, a system with a high level of concern for access method, a low level of concern for backend connections, and a low level of concern for the number of authorized users would have a high level of concern for external system exposure. Table 3.2 provides guidance to agencies in assigning values to the level of concern for external system exposure.

TABLE 3.2 LEVELS OF CONCERN FOR EXTERNAL EXPOSURE

	ACCESS METHOD	BACK-END CONNECTIONS	NUMBER OF USERS
LOW	Access to the system is via protected communications channels, (e.g., dedicated connections).	No backend connections to any systems exist.	An extremely limited number of authorized individuals have access to the system.
MODERATE	Access to the system is via relatively constrained communications channels, (e.g., intranet connection).	A backend connection to a system exists which itself has relatively constrained connections to other systems (e.g., intranet connections).	A limited number of authorized individuals have access to the system.
HIGH	Access to the system is via freely accessible communications channels, (e.g., Internet, or wireless networks).	A backend connection to a system exists which itself has freely accessible connections to other systems, (e.g., Internet or wireless networks).	An unlimited number of authorized individuals have access to the system, (e.g., a public kiosk).

3.1.3.2 Internal System Exposure

Internal system exposure should only be considered for systems where there is a high level of concern for confidentiality. Consider the potential exposure of the IT system to internal threats, (i.e., individuals without proper security background assurances and/or clearances, access approvals, and/or need-to-know, gain access to highly sensitive (unclassified) information or (classified) national security information).[15] To determine the appropriate level of concern for internal system exposure, refer to Table 3.3. There are four cases listed in the table that characterize the possible states of the system with regard to authorized users and information being accessed. Select the case that most appropriately describes the system's state. A corresponding value, (i.e., low, moderate, or high) can be assigned representing the level of concern for internal exposure to the system. For example, if all users with access to a system processing, storing, or transmitting (classified) national security information or highly sensitive (unclassified) information have ap-

15. The concepts of clearance, access approval, and need-to-know are generally associated with (classified) national security information and systems. However, agencies processing, storing, and transmitting highly sensitive unclassified information, (i.e., information engendering a high level of concern for confidentiality), will employ similar concepts analogous to those used in the classified environment. Note that the use of the word clearance in this special publication refers to either an individual security background assurance (sometimes called a security check) or a formal security clearance (as is accomplished for access to classified information). For example, system managers of important Federal unclassified systems are typically required to undergo a background check (even though there is no need to access classified information) because of the potential for harm to an agency's operations.

propriate security background assurances and/or clearances, formal access approvals, and need-to-know, this would equate to Case #1 and engender a low level of concern for internal exposure.

TABLE 3.3 LEVELS OF CONCERN FOR INTERNAL EXPOSURE

	CLEARANCE	ACCESS APPROVAL	NEED-TO-KNOW
LOW CASE 1	Each user has a clearance for **all information** processed, stored or transmitted by the system.	Each user has access approval for **all information** processed, stored or transmitted by the system.	Each user has a valid need-to-know, for **all information** processed, stored or transmitted by the system.
MODERATE CASE 2	Each user has a clearance for **all information** processed, stored or transmitted by the system.	Each user has access approval for **all information** processed, stored or transmitted by the system.	Each user has a valid need-to-know, for **some information** processed, stored or transmitted by the system.
MODERATE CASE 3	Each user has a clearance for the **most sensitive information** processed, stored or transmitted by the system.	Each user has access approval for only that **information for which the user is to have access**.	Each user has a valid need-to-know for that **information which the user is to have access**.
HIGH CASE 4	Some users do not have a clearance for **all information** processed, stored or transmitted by the system. Each user has a clearance for that **information which the user is to have access**.	Each user has access approval for only that **information for which the user is to have access**.	Each user has a valid need-to-know for that **information which the user is to have access**.

3.2 Security Controls

Security controls have been included in a companion publication, NIST Special Publication 800-53, *Minimum Security Controls for Federal Information Technology Systems* (projected for Spring 2003), separated from the C&A process description, in anticipation that the set of controls will evolve over time as technology changes and new safeguards for IT systems are identified. The following sections describe: (1) the security control organization and naming convention, (2) the process of selecting security controls, and (3) the process of adjusting the security controls based on risk-based decisions by the agency.

3.2.1 ORGANIZATION OF SECURITY CONTROLS

The security controls in Special Publication 800-53 are organized into *classes* and *families* for ease of use. There are three general classes of security controls, (i.e., management, operational, and technical), which correspond to the major sections of a security plan as defined by NIST Special Publication 800-18. Within each of the classes, specific families are defined covering the following topic areas: risk management, system development and acquisition, configuration management, system interconnection, personnel security, security awareness, education, and training, physical and environmental protection, media protection, contingency planning, hardware and system software maintenance, system and data integrity, documentation, incident response capability, identification and authentication, logical access, audit, and communications. The security controls are grouped within the families by *critical elements*. Critical elements, as explained in NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology*

Systems, represent important security-related focus areas for the system with each critical element addressed by one or more security controls. For example, a critical element in the Identification and Authentication family states that: "USERS ARE INDIVIDUALLY AUTHENTICATED VIA PASSWORDS, TOKENS, OR OTHER DEVICES." Several security controls in the identification and authentication family are associated with the above critical element. These subordinate controls must be shown to be correctly implemented and effective to demonstrate that the critical element has been satisfied.

A unique naming convention for security controls is employed to help describe, in shorthand form, the family from which the control is selected and the number of the control within the family. For the controls (supporting higher levels of concern for confidentiality, integrity, and availability) targeted for inclusion in a supplemental package, additional designators are used as extensions to the basic names. The level of concern designator indicates either M for moderate or H for high. The security factor designator indicates C for confidentiality, I for integrity, and/or A for availability. For example, a security control identified as PS-8 indicates that the control is from the personnel security family and is the eighth such control in that family. A more advanced control from the same family, PS-8.MCIA, is appropriate for systems requiring moderate confidentiality, integrity, and availability. In another example, a security control with an LA-16.HCI designator indicates that the control is from the logical access control family (the sixteenth such control in that family) and is appropriate for systems requiring high confidentiality and integrity. By definition, security controls not supporting higher levels of concern, are contained in the standard package and do not use any extension designators since the controls are all applicable to basic levels of confidentiality, integrity, and availability. Figure 3.1 illustrates the naming convention for security controls and the key sections of the nomenclature.

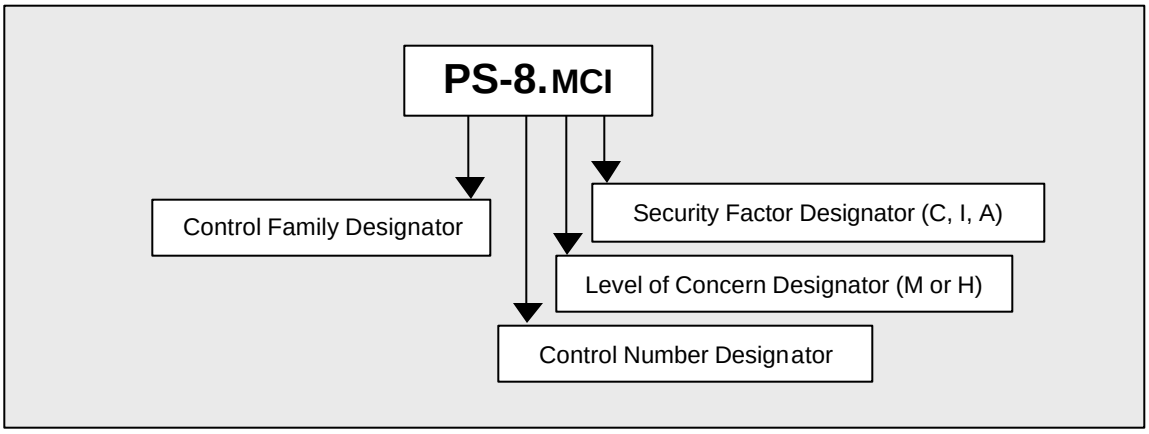

FIGURE 3.1 NAMING CONVENTION FOR SECURITY CONTROLS

3.2.2 SECURITY CONTROL SELECTION

After the particular levels of concern for confidentiality, integrity, availability, and system exposure have been determined, the appropriate security controls can be selected from the pre-defined controls provided in NIST Special Publication 800-53, *Minimum Security Controls for Federal Information Technology Systems* (projected for Spring 2003). The security controls contained in the special publication are the minimum security controls recommended for federal systems requiring basic, moderate, or high degrees of protection in the areas of confidentiality, integrity, and availability. When other national, agency or component level policy documents prescribe IT system security requirements that are not adequately covered by or that are more restricted than the applicable security controls included in NIST Special Publication 800-53, additional controls

meeting these requirements must be added to the security controls selected for the particular IT system undergoing C&A.

The process of selecting the appropriate security controls is typically accomplished in three steps: (1) the selection of the standard package of security controls, (2) the creation of a specialized set of supplemental security controls based on stated higher levels of concern for confidentiality, integrity, and availability, and (3) adding agency-specific or technology-driven security controls. The standard package of security controls includes basic-level controls for confidentiality, integrity, and availability. This is the baseline set of security controls that should be implemented in all federal IT systems. After the standard package of security controls is selected, it is necessary to examine the stated levels of concern for confidentiality, integrity, and availability to determine if there is a need to bring in additional controls for the system in a supplemental package.

A careful review of the available supplemental controls in NIST Special Publication 800-53 should be accomplished to select the appropriate security controls for the supplemental package. To ensure completeness in the review and selection process, each family within the management, operational, and technical control classes should be examined. For example, an agency with a stated moderate level of concern for confidentiality, high level of concern for integrity, and low level of concern for availability, (i.e., C=M, I=H, A=L), would select the standard package of basic controls and then look through each family for applicable controls with any of the following extensions to the basic control name: MC, MCI, MCA, MCIA, HI, HCI, HIA, HCIA. This process ensures that every security control addressing moderate confidentiality and high integrity is selected for the supplemental package. Controls for low availability are covered in the standard package of basic controls. Figure 3.2 illustrates the security control selection process for the standard and supplemental packages.

FIGURE 3.2 SECURITY CONTROL SELECTION PROCESS

The documented levels of concern for internal and external system exposure can have an effect on the certification level selected for the system and can also provide justification for management-approved substitution of equivalent controls or granting waivers for selected security controls. The effect of internal and external system exposure on the certification level and security controls selected is described in Sections 3.2.3 and 3.3.5.

3.2.3 SECURITY CONTROL SELECTION ADJUSTMENT

There may be certain occasions when management makes a risk-based decision to substitute equivalent controls, waive security controls, or enhance the recommended security controls for an IT system. For example, management may approve the substitution of equivalent security controls if justified for operational, cost, or other reasons (provided the security objective is still achieved). This management-approved substitution of equivalent controls should be documented in the security plan. Management may choose to grant a waiver for specific security controls because the benefits of operating without the controls (at least temporarily) outweigh the risk of waiting for full control implementation. If specific security controls are waived, this should also be noted in the security plan with complete rationale and supporting documentation of the degree to which the remaining security controls compensate for the controls that have not been implemented. Alternatively, there may be times when management implements more stringent security controls than are contained in the standard and supplemental packages. This too, should be documented in the security plan.

To better illustrate the waiver process, the following example is provided. An agency having a high level of concern for confidentiality due to the criticality/sensitivity of the information being processed, stored, or transmitted by the system would initially select the security controls for high confidentiality from NIST Special Publication 800-53. Upon further analysis, the agency determines that the level of concern for both internal and external system exposure is low, (i.e., the system has no external network connections, the system is located in a highly protected facility with guards and perimeter fencing, and all individuals accessing the system have appropriate authorizations to access the information on the system). Selected technical controls involving strong operating system access controls and certain encryption controls contained in the supplemental package may, at the discretion of management, be waived provided there are other compensating security controls, (i.e., management and operational controls) which provide the needed protection for the system to keep the residual risk within an acceptable range.

3.2.4 SUMMARY OF SECURITY CONTROL SELECTION

In summary, selecting the appropriate security controls for the IT system is a three-step process:

STEP 1: CHARACTERIZE THE SYSTEM

Obtain the following system-related information from the security plan:

- Accreditation boundary for the system and, if appropriate, the proposed decomposition of the system into subsystem components.
- Criticality/sensitivity of the system (or subsystems, if appropriate) based on levels of concern for confidentiality, integrity and availability. [Table 3.1]
- External system exposure based on level of concern by system or by subsystem, if appropriate. [Table 3.2]
- Internal system exposure based on level of concern by system or by subsystem, if appropriate. [Table 3.3]

STEP 2: SELECT THE APPROPRIATE MINIMUM SECURITY CONTROLS FOR THE SYSTEM

- Select minimum security controls from the standard package of basic controls (mandatory for all systems). [NIST Special Publication 800-53]

- Select additional minimum security controls (moderate/high levels), if appropriate, to create a supplemental package of controls based on increased levels of concern for confidentiality, integrity, and/or availability. [NIST Special Publication 800-53]
- Create agency-specific or technology-driven security controls. [If needed security controls are not available in NIST Special Publication 800-53]

STEP 3: ADJUST SECURITY CONTROLS BASED ON SYSTEM EXPOSURE AND RISK DECISIONS

- Adjust the selected controls based on internal/external exposure and risk based decisions; describe the controls in documented, allowable waivers.

3.3 Security Certification Levels

The fundamental purpose of the certification process is to determine if the security controls for the IT system are correctly implemented and are effective in their application. The correct and effective implementation of these controls provides assurance that the system security requirements have been satisfied. There are many *verification techniques* that can be employed during the C&A process to determine the correctness and effectiveness of the security controls. These techniques include:

- Interviewing agency personnel associated with the security aspects of the system;
- Reviewing and examining security-related policies, procedures, and documentation;
- Observing security-related activities and operations;
- Analyzing, testing, and evaluating the security relevant and security critical aspects of system hardware, software, firmware, and operations; and
- Conducting demonstrations and exercises.

There are three certification levels defined in this special publication: Security Certification Level 1 (SCL-1), Security Certification Level 2 (SCL-2), and Security Certification Level 3 (SCL-3). Each of the successive certification levels provides additional rigor and intensity in the application of the verification techniques to determine compliance with the security requirements and to demonstrate the correctness and effectiveness of the security controls. The following sections describe the certification levels and the verification techniques associated with those levels.

3.3.1 SECURITY CERTIFICATION LEVEL 1

SCL-1 is the *entry-level* certification for IT systems. This certification level is appropriate for systems engendering low levels of concern for confidentiality, integrity, and availability. It is also appropriate, at the discretion of management, for systems with moderate to high levels of concern for confidentiality, integrity, and/or availability *and* low to moderate levels of concern for system exposure, (i.e., systems operating in low to moderate risk environments). SCL-1 certifications typically employ agency-directed, independent assessments or basic security reviews of IT systems using questionnaires or specialized checklists. These assessments are intended to demonstrate at relatively low levels of assurance that the security controls for IT systems are correctly implemented and are effective in their application. SCL-1 certifications are relatively low intensity endeavors that can be accomplished with minimal resources using simple verification techniques such as personnel interviews, documentation reviews, and observations.

3.3.2 SECURITY CERTIFICATION LEVEL 2

SCL-2 is the *mid-level* certification for IT systems. This certification level is appropriate for systems engendering *moderate* levels of concern for confidentiality, integrity, and/or availability. It may also be appropriate, at the discretion of management, for systems with high levels of concern for confidentiality, integrity, and/or availability *and* low to moderate levels of concern for system exposure, (i.e., systems operating in low to moderate risk environments). SCL-2 certifications call for independent assessments of IT systems building on the verification techniques and procedures from SCL-1 and adding more substantial techniques and procedures, as appropriate. These independent assessments are intended to demonstrate at moderate levels of assurance that the security controls are correctly implemented and are effective in their application. SCL-2 certifications are moderate intensity endeavors that can be accomplished with limited to moderate resources using standard, commercially available, assessment tools and verification techniques such as personnel interviews, documentation reviews, observations, demonstrations, and limited ST&E activities, (e.g., limited functional testing, regression analysis and testing, and optional penetration testing).

3.3.3 SECURITY CERTIFICATION LEVEL 3

SCL-3 is the *top-level* certification for IT systems. This certification level is appropriate for systems engendering *high* levels of concern for confidentiality, integrity, and/or availability. SCL-3 certifications call for independent assessments of IT systems building on the verification techniques and procedures from SCL-1 and SCL-2 and employing the most rigorous verification techniques, as appropriate. These independent assessments are intended to demonstrate, at high levels of assurance, that the security controls for IT systems are correctly implemented and are effective in their application. SCL-3 certifications are high intensity endeavors that can be accomplished with substantial resources using the most advanced assessment tools and verification techniques available, (i.e., system design analysis, extended functional testing with test coverage analysis, regression analysis/testing, demonstrations, exercises, and penetration testing with Red Team option). Table 3.4 summarizes the different verification techniques by certification level.

TABLE 3.4 CERTIFICATION LEVELS AND VERIFICATION TECHNIQUES

SCL	VERIFICATION TECHNIQUES
SCL-3	▪ **High intensity**, exercised-based, independent assessment ▪ System design analysis ▪ Functional testing with coverage analysis ▪ Regression analysis and regression testing ▪ Penetration testing (Red Team optional) ▪ Demonstrations and exercises to verify security control correctness and effectiveness ▪ SCL-1 and SCL-2 verification techniques (if appropriate)
SCL-2	▪ **Moderate intensity**, demonstration-based, independent assessment ▪ Functional testing ▪ Regression analysis and regression testing ▪ Penetration testing (optional) ▪ Demonstrations to verify security control correctness and effectiveness ▪ SCL-1 verification techniques (if appropriate)
SCL-1	• **Low intensity**, checklist-based, independent security review • Interview of personnel • Review of system-related security policies, procedures, documents • Observation of system operations and security controls

3.3.4 CERTIFICATION LEVEL SELECTION

After the particular levels of concern for confidentiality, integrity, and availability have been determined, the initial certification level can be selected. If any level of concern for confidentiality, integrity, or availability is high, then certification level three (SCL-3) is selected. If there are no high levels of concern, and if any level of concern for confidentiality, integrity and availability is moderate, then certification level two (SCL-2) is selected. If all levels of concern for confidentiality, integrity, and availability are low, then certification level one (SCL-1) is selected. Once the initial certification level has been selected, the level can be adjusted based on the level of concern for system exposure to obtain the actual certification level.

If the level of concern for confidentiality is low or moderate, only external system exposure is considered in making possible adjustments to the initial certification level. If the level of concern for external system exposure is high, then no adjustments to the certification level are necessary. If the level of concern for external system exposure is moderate, then the initial certification level can be lowered by one level at the discretion of management, (e.g., SCL-3 downgraded to SCL-2 or SCL-2 downgraded to SCL-1). If the level of concern for external system exposure is low, then the initial certification level can be lowered by up to two levels at the discretion of management, (e.g., SCL-3 downgraded to SCL-2 or SCL-1, SCL-2 downgraded to SCL-1).

If the level of concern for confidentiality is high, then both external and internal system exposure are considered in making possible adjustments to the initial certification level. To determine the total system exposure, consult Table 3.5. Find the appropriate row in the table that reflects the level of concern for external and internal system exposure—then obtain the level of concern for total system exposure from the last column in that row.

TABLE 3.5 DETERMINING TOTAL SYSTEM EXPOSURE

EXTERNAL SYSTEM EXPOSURE	INTERNAL SYSTEM EXPOSURE	TOTAL SYSTEM EXPOSURE
LOW	LOW	LOW
LOW	MODERATE	MODERATE
LOW	HIGH	HIGH
MODERATE	LOW	MODERATE
MODERATE	MODERATE	MODERATE
MODERATE	HIGH	HIGH
HIGH	LOW	HIGH
HIGH	MODERATE	HIGH
HIGH	HIGH	HIGH

If the level of concern for total system exposure is high, then no adjustments to the initial certification level are necessary. If the level of concern for total system exposure is moderate, then the initial certification level can be lowered by one level at the discretion of management, (e.g., SCL-3 downgraded to SCL-2 or SCL-2 downgraded to SCL-1). If the level of concern for total system exposure is low, then the initial certification level can be lowered by up to two levels at the discretion of management, (e.g., SCL-3 downgraded to SCL-2 or SCL-1, SCL-2 downgraded to SCL-1).

3.3.5 SUMMARY OF CERTIFICATION LEVEL SELECTION

In summary, selecting the certification level for the IT system is a three-step process:

STEP 1: CHARACTERIZE THE SYSTEM

Obtain the following system-related information from the security plan:

- Accreditation boundary for the system and, if appropriate, the proposed decomposition of the system into subsystem components.
- Criticality/sensitivity of the system (or subsystems, if appropriate) based on levels of concern for confidentiality, integrity and availability. [Table 3.1]
- External system exposure based on level of concern by system or by subsystem, if appropriate. [Table 3.2]
- Internal system exposure (confidentiality only) based on level of concern by system or by subsystem, if appropriate. [Table 3.3]

STEP 2: SELECT THE APPROPRIATE INITIAL SECURITY CERTIFICATION LEVEL FOR THE SYSTEM

- If **any** level of concern for confidentiality, integrity, or availability = **HIGH**

  Then **Select SCL-3**

  Otherwise

- If **any** level of concern for confidentiality, integrity, or availability = **MODERATE**

  Then **Select SCL-2**

  Otherwise

- If all levels of concern for confidentiality, integrity, and availability = **LOW**

  Then **Select SCL-1**

STEP 3: ADJUST SECURITY CERTIFICATION LEVEL BASED ON SYSTEM EXPOSURE

- If the level of concern for confidentiality and/or integrity = **HIGH**

  Then **proceed directly to Step 3B.**

  Otherwise

  Proceed to Step 3A and skip Step 3B.

STEP 3A: CONSIDER EXTERNAL EXPOSURE TO ADJUST CERTIFICATION LEVEL

- If the level of concern for external system exposure = **HIGH**

  Then **No adjustments to the certification level are necessary**

  Otherwise

- If the level of concern for external system exposure = **MODERATE**

  And if the initial certification level from Step 3 = **SCL-3**

  Then **Option to reduce certification level to SCL-2 at the discretion of management**

  Otherwise

- If the level of concern for external system exposure = **MODERATE**

  And if the initial certification level from Step 3 = **SCL-2**

  Then **Option to reduce certification level to SCL-1 at the discretion of management**

  Otherwise

- If the level of concern for external system exposure = **LOW**

  And if the initial certification level from Step 3 = **SCL-3**

  Then **Option to reduce certification level to SCL-2 or SCL-1 at the discretion of management**

  Otherwise

- If the level of concern for external system exposure = **LOW**

  And if the initial certification level from Step 3 = **SCL-2**

  Then **Option to reduce certification level to SCL-1 at the discretion of management**

STEP 3B: CONSIDER INTERNAL AND EXTERNAL EXPOSURE TO ADJUST CERTIFICATION LEVEL

- Consult Table 3.5 to determine the level of concern for total system exposure. Find the appropriate row in the table that reflects the level of concern for external and internal system exposure—then obtain the level of concern for total system exposure from the last column in that row.

- If the level of concern for total system exposure = **HIGH**

  Then **No adjustments to the certification level are necessary**

  Otherwise

- If the level of concern for total system exposure = **MODERATE**

  And if the initial certification level from Step 3 = **SCL-3**

  Then **Option to reduce certification level to SCL-2 at the discretion of management**

  Otherwise

- If the level of concern for total system exposure = **MODERATE**

  And if the initial certification level from Step 3 = **SCL-2**

  Then **Option to reduce certification level to SCL-1 at the discretion of management**

  Otherwise

- If the level of concern for total system exposure = **LOW**

  And if the initial certification level from Step 3 = **SCL-3**

  Then **Option to reduce certification level to SCL-2 or SCL-1 at the discretion of management**

  Otherwise

- If the level of concern for total system exposure = **LOW**

  And if the initial certification level from Step 3 = **SCL-2**

  Then **Option to reduce certification level to SCL-1 at the discretion of management**

Reducing the certification level after careful consideration of external and internal system exposure is a risk-based decision that may be taken by management. Consider the following examples:

Example 1: A federal IT system processes, stores, and transmits information for a key financial application. The agency responsible for the system determines that the level of concern for integrity is high, and the levels of concern for confidentiality and availability are moderate. The agency also determines that the level of concern for external system exposure is moderate due to the fact that access to the financial system is via relatively constrained communications channels, (i.e., intranet connection), there are no backend connections to the system, and the number of users is relatively small (confined only to staff members in the section responsible for the application). Internal system exposure is not considered since the level of concern for confidentiality is not high. Based on the above information, the standard package of security controls and a supplemental package of controls for moderate confidentiality, high integrity, and moderate availability are identified for the system. The high level of concern for integrity targets the certification level initially at SCL-3. However, after assessing all of the relevant information, management decides to reduce the certification level to SCL-2 due to the moderate level of concern for external system exposure.

Example 2: A federal IT system processes, stores, and transmits (classified) national security information for a military intelligence application. The agency responsible for the system determines that the level of concern for confidentiality is high and the levels of concern for integrity and availability are moderate. The agency also determines that the level of concern for external system exposure is low due to the fact that all access to the system is via protected communications channels, (i.e., dedicated lines), there are no backend connections to the system, and the number of users is very small (confined only to staff members in the section responsible for the application). Internal system exposure is also judged to be low due to the fact that all personnel having access to the system have appropriate security clearances, formal access approvals, and need-to-know. Based on the above information, the standard package of security controls and a supplemental package of controls for high confidentiality, moderate integrity, and moderate availability are identified for the system. Consulting Table 3.5, the low levels of concern for both internal and external system exposure produce a low level of concern for total system exposure. The high level of concern for confidentiality targets the certification level initially at SCL-3. However, after assessing all of the relevant information, management decides to reduce the certification level to SCL-1 due to the low level of concern for total system exposure.

3.3.6 RELATING SECURITY CONTROLS TO THE CERTIFICATION LEVELS

It is important to understand the relationship between *certification levels* and *security controls*. The certification level and security controls selected for the IT system are both based on the stated levels of concern for confidentiality, integrity, and availability. The level of concern for system exposure can affect the initial selection of the certification level and the security controls as illustrated in the previous sections. The standard package of security controls and the agency-defined, supplemental package of controls, provide the minimum security controls for IT systems in the areas of confidentiality, integrity, and availability for low, moderate, and high levels of concern. The fundamental concept is that as the level of concern increases above the lowest level in confidentiality, integrity, or availability, additional security controls are brought in at the discretion of the agency and the rigor and intensity of the certification process is increased accordingly—committing more resources to certifying systems having greater levels of concern and more robust security controls.

3.4 Security Control Verification

Each security control associated with a critical element in NIST Special Publication 800-53 has, associated with it, verification techniques and procedures. Verification techniques are determined by the selected SCL as illustrated in Table 3.4. Verification procedures describe the specific assessment activities carried out by the certifier and the certification team to demonstrate the correct and effective implementation of security controls. NIST Special Publication 800-53A, *Techniques and Procedures for the Verification of Security Controls in Federal Information Technology Systems* (projected for Spring 2003), provides a complete listing of the standardized verification techniques and procedures for the security controls contained in NIST Special Publication 800-53. Table 3.6 illustrates a simple example of verification techniques and procedures for selected security controls within the I&A family. A special section in the table is reserved for verification techniques and procedures applicable to developmental systems.

TABLE 3.6 SECURITY CONTROLS AND VERIFICATION PROCEDURES

CLASS: TECHNICAL		**FAMILY: IDENTIFICATION AND AUTHENTICATION (IA)**	
CRITICAL ELEMENT: Passwords, tokens, or other devices are used to identify and authenticate users.			
SECURITY CONTROL	**SCL-1**	**SCL-2**	**SCL-3**
IA-1: A current list of authorized users and their access is maintained and approved.	*Developmental ST&E:* • Not applicable. *Operational ST&E:* • **Review** policies and procedures for user authorization.	*Developmental ST&E:* • Not applicable. *Operational ST&E:* • **Examine** list of authorized users and their access.	*Developmental ST&E:* • Not applicable. *Operational ST&E:* • **Examine** system access control list and compare with written list of authorized users.
IA-2: Passwords for the IT system are changed at least every ninety days or earlier if needed.	*Developmental ST&E:* • Not applicable. *Operational ST&E:* • **Review** policies and procedures for password management. • **Interview** users to determine familiarity with password changing policies and procedures.	*Developmental ST&E:* • Not applicable. *Operational ST&E:* • **Observe** users changing passwords.	*Developmental ST&E:* • Not applicable. *Operational ST&E:* • **Examine** the password file using audit software to verify that the passwords have been changed within the specified ninety-day timeframe.
IA-5: Vendor-supplied passwords are replaced immediately.	*Developmental ST&E:* • Not applicable. *Operational ST&E:* • **Review** policies and procedures for vendor-supplied password replacement. • **Interview** system administrators to determine their familiarity with password replacement policies and procedures.	*Developmental ST&E:* • Not applicable. *Operational ST&E:* • **Demonstrate** that vendor-supplied passwords have been removed by attempting to log on using common vendor passwords.	*Developmental ST&E:* • **Review** administrator guidance for vendor-supplied password replacement. *Operational ST&E:* • **Examine** the password file using audit software to verify that vendor-supplied passwords have been removed from the system.

In most cases, the verification procedures are cumulative, that is, the procedures employed at a particular SCL include the procedures from the next lower level. In practice, a certifier would use the suggested verification procedures from NIST Special Publication 800-53A as the starting point for developing more specific ST&E procedures, which may, in certain cases, need to be developed based on a particular platform. For example, a testing plan derived from the verification procedures for security control IA-5 from the example in Figure 3.6 would provide specific step-by-step guidance on trying to log on to a Windows 2000-based system or a Unix-based system. This additional specificity in the ST&E procedures provides greater consistency and repeatability of testing from certifier to certifier.

As explained in NIST Special Publication 800-18, verification activities should be independent of the manager responsible for the major application or general support system. Independent verifications can be internal or external but should be performed by individuals or organizations free from personal and external factors that could impair their independence or their perceived independence, (e.g., they designed the system under review).

CHAPTER FOUR

CERTIFICATION AND ACCREDITATION PROCESS

4

PHASES AND ACTIVITIES

Security assurance is the degree of confidence one has that the managerial, technical, and operational security controls work as intended to protect the IT system and the information it processes, stores, and transmits…

The C&A process defined in this special publication consists of four distinct phases, *pre-certification*, *certification*, *accreditation*, and *post-accreditation*. Each of these phases is addressed in every system accreditation (for both operational legacy systems and new development systems) irrespective of where the system is in the life cycle process. Figure 4.1 illustrates the four phases of the C&A process and the specific tasks associated with each phase. Each of these phases is described in greater detail in the following sections.

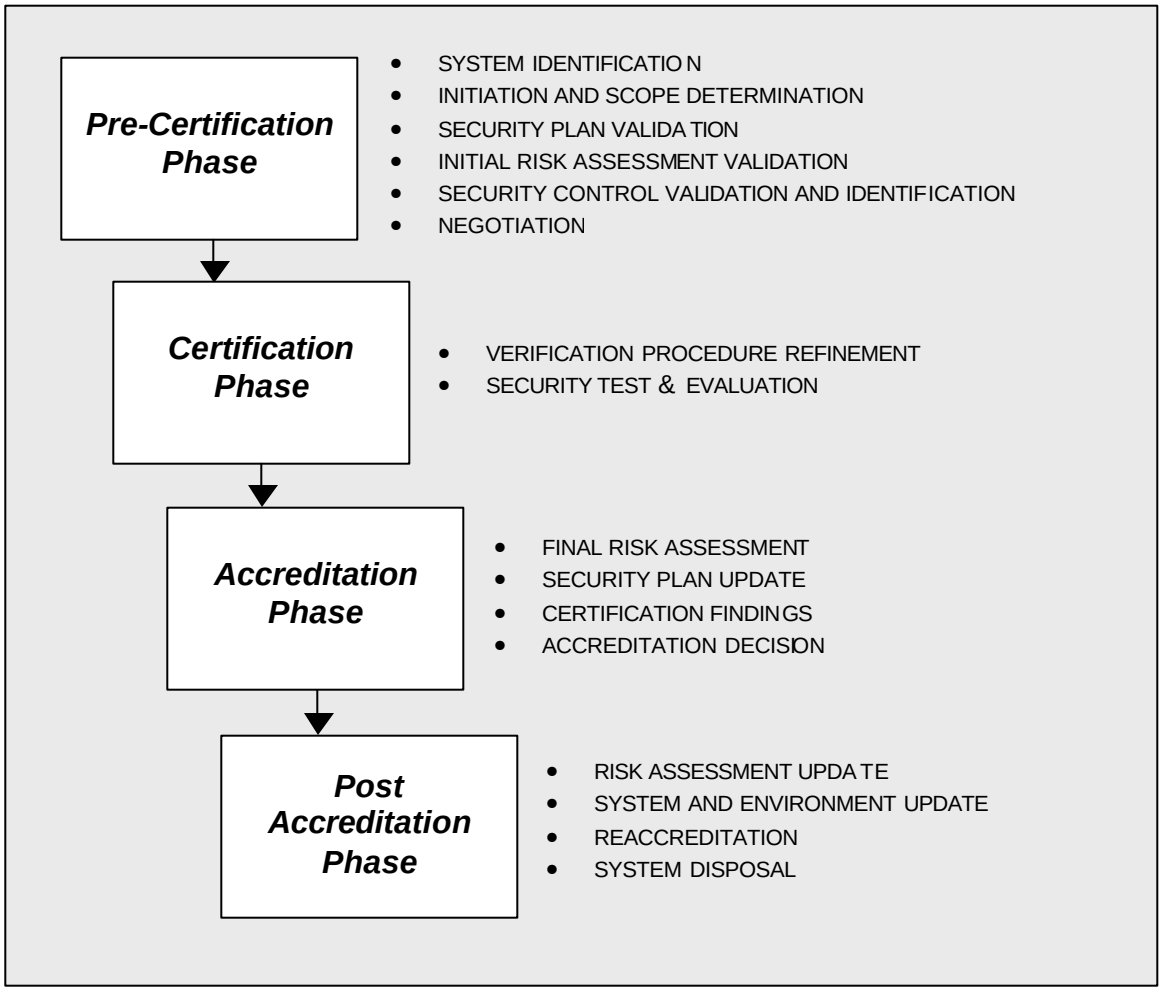

FIGURE 4.1 CERTIFICATION AND ACCREDITATION PHASES AND ACTIVITIES

4.1 Pre-Certification Phase

The purpose of the pre-certification phase is to prepare for the verification activities that will take place during the certification phase. The pre-certification phase consists of six tasks:

- System Identification;
- Initiation and Scope Determination;
- Security Plan Validation;
- Initial Risk Assessment Validation;
- Security Control Validation and Identification; and
- Negotiation.

A significant portion of the information needed to complete the pre-certification tasks and subtasks can be obtained from current agency security plans, risk assessments, or other security related documentation. If security plans and risk assessments have not yet been completed by the agency, it is recommended that those activities be completed prior to proceeding with the C&A process. NIST Special Publications 800-18 and 800-30 provide guidance to agencies on preparing security plans and conducting risk assessments. Upon completion of the pre-certification phase, the C&A process proceeds with the certification phase. The following sections contain descriptions of all pre-certification tasks and associated subtasks.

TASK 1: SYSTEM IDENTIFICATION

The objective of this task is to validate that the security plan contains essential system identification information. System identification information includes such items as system name, responsible organization, contact information, responsible individuals, system boundary, and status.

SYSTEM NAME/TITLE

SUBTASK 1.1: Validate that the security plan lists the name of the system and provides a unique identifier for the system.

REFERENCE: [NIST Special Publication 800-18]

RESPONSIBLE ORGANIZATION

SUBTASK 1.2: Validate that the security plan lists the name and location of the agency responsible for the system and the organizations containing the end users of the system.

REFERENCE: [NIST Special Publication 800-18]

CONTACT INFORMATION

SUBTASK 1.3: Validate that the security plan lists the name, title, and contact information (i.e., address, telephone number, facsimile number, and electronic mail address) of the program manager, system owner, or person(s) knowledgeable about the system.

REFERENCE: [NIST Special Publication 800-18]

ASSIGNMENT OF SECURITY RESPONSIBILITY

SUBTASK 1.4: Validate that the security plan lists the name, title, address, and telephone number of the person(s) responsible for security of the system.

REFERENCE: [NIST Special Publication 800-18]

SYSTEM BOUNDARY

SUBTASK 1.5: Validate that the security plan describes the boundary of the system for purposes of accreditation.

ADVISORY NOTE: As the number and complexity of IT systems increase, the confusion over areas of responsibility for system components also increases. Various authorities will have responsibility for different parts of the system, such as the actual communications components (e.g., communications lines, switches, routers), host computers, shared devices on the network (e.g., printers, servers), and the end-user terminals or workstations. During the security certification of these complex systems, the boundary and the responsibility for certification of each area must be clearly defined and documented in the security plan to ensure that the entire system is covered in the effort. The description includes diagrams or text to clearly delineate which components are to be evaluated as part of the certification process. All components included are described in the systems description. Elements outside of the accreditation boundary are included in the section on external interfaces. A good rule to use in determining the accreditation boundary is that the DAA typically has budgetary and operational control over the system being certified and accredited.

REFERENCE: [NIST Special Publications 800-18, 800-37 Section 2.5]

SYSTEM STATUS

SUBTASK 1.6: Validate that the security plan describes where the system is in the system development life cycle, (i.e., initiation phase, development/acquisition phase, implementation phase, operation/maintenance phase, disposal phase), and lists the status of existing documentation, development and implementation schedule, milestones, and costs.

REFERENCE: [NIST Special Publication 800-18]

TASK 2: INITIATION AND SCOPE DETERMINATION

The objective of this task is to initiate the C&A process and to determine the scope of the certification effort. Typically, the C&A process is initiated by holding a series of meetings with key participants—the DAA, program manager, system owner, certifier, system security officer, and any other individuals within the agency who have an interest in certifying and accrediting the IT system. This initial series of meetings is critical to establishing the necessary communication among all participants in the C&A process. Participants share their initial thoughts on various aspects of the C&A process to include: (1) the levels of concern for confidentiality, integrity, and availability, (i.e., the system criticality/sensitivity), (2) the levels of concern for both external and internal system exposure, and (3) the security certification level. General agreement is reached on these key issues upon completion of this task.

SYSTEM CRITICALITY/SENSITIVITY

SUBTASK 2.1: Validate that the security plan accurately describes the criticality/sensitivity of the IT system with respect to the agency's mission responsibilities.

ADVISORY NOTE: System criticality/sensitivity is a measure of the importance and nature of the information processed, stored, and transmitted by the IT system to the agency's mission and day-to-day operations. The criticality/sensitivity of an IT system and its information can be addressed by analyzing what the data/system owner or program manager defined as the system requirements for confidentiality, integrity, and availability. System *confidentiality* provides assurance that the information in an IT system is protected from disclosure to unauthorized persons, processes, or devices. System *integrity* provides assurance that information in an IT system is protected from unauthorized, unanticipated, or unintentional modification or destruction. System integrity also addresses the quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. System

availability provides assurance that information and IT system resources are accessible to authorized users and/or system-related processes on a timely and reliable basis and are protected from denial of service. By performing this analysis, the value of the system can be validated. The value is one of the major factors in risk management.

REFERENCES: [NIST Special Publications 800-18, 800-30, 800-37 Section 3.1.1]

SYSTEM EXPOSURE

SUBTASK 2.2: Validate that the security plan accurately describes the external and internal exposure of the IT system.

ADVISORY NOTE: System exposure is a measure of the potential risk to an IT system from both external and internal threats. *External system exposure* relates to: (1) the method by which users access the system, (2) the existence of backend connections to the system and to what the backend systems are connected, and (3) the number of users that access the system. *Internal system exposure* relates to the types of individuals that have authorization to access the system and the information the system stores, processes, and transmits. It includes such items as individual clearance levels, access approvals, and need-to-know. Internal system exposure is considered for IT systems that are processing, storing, or transmitting (classified) national security information or (unclassified) sensitive information with a high level of concern for confidentiality. External system exposure is also considered for IT systems with a high level of concern for integrity.

REFERENCES: [NIST Special Publications 800-37 Sections 3.1.2, 3.1.3]

SECURITY CERTIFICATION LEVEL

SUBTASK 2.3: Select the security certification level, (i.e., SCL-1, SCL-2, or SCL-3) for the IT system; or for large and complex systems, select the security certification level for all subsystem-level components within the accreditation boundary.

ADVISORY NOTE: There are three steps in selecting the SCL: (1) characterize the IT system, (2) select the initial SCL, and (3) adjust the initial SCL based on the levels of concern for external system exposure and, if appropriate, internal system exposure.

REFERENCES: [NIST Special Publications 800-37 Sections 3.1, 3.3.5]

TASK 3: SECURITY PLAN VALIDATION

The objective of this task is to validate that the security plan: (1) provides a full and accurate description of the IT system and the system's operating environment, (2) identifies the security requirements for the system, and (3) delineates responsibilities and expected behavior of individuals who access the system. The system description includes mission, functions, and capabilities. A high level overview of the system architecture (hardware, software, firmware and associated interfaces) is also provided along with a description of the facility where the system resides and the responsible organizations and individuals assigned to operate the system. The security requirements articulate the types and levels of protection necessary for equipment, data, information, applications, and facilities to meet applicable laws, directives, regulations, standards, instructions and/or security policies. The security controls include the management, operational, and technical safeguards employed to protect the information in the IT system.

GENERAL DESCRIPTION AND PURPOSE

SUBTASK 3.1: Validate that the security plan describes, in general terms, the purpose, function, and capabilities of the system and the information processed, stored, and transmitted.

ADVISORY NOTE: The general description lists all applications supported by the system and a functional description and purpose of each supported application. Functional diagrams and processing flows from system input to system output are included in the sys-

tem description. If a system concept of operations exists, it is either referenced or included as an appendix to the system security plan.

REFERENCE: [NIST Special Publication 800-18]

SUBTASK 3.2: Validate that the security plan lists all user organizations, both internal and external, identifies any system users who are not U.S. citizens, if applicable, and identifies the type of information and processing provided.

REFERENCE: [NIST Special Publication 800-18]

SUBTASK 3.3: Validate that the security plan describes the user's access rights or clearances to the information processed, stored or transmitted by the IT system including any privileged roles and privileged users for the system.

ADVISORY NOTE: A system's authorized users may include both government and contractor personnel. If proprietary information from commercial organizations other than the users will be processed, stored, or transmitted, sufficient controls are designed into the system to prevent the contractor personnel from gaining intentional or unintentional access to the proprietary information.

REFERENCE: [NIST Special Publication 800-18]

SYSTEM ENVIRONMENT

SUBTASK 3.4: Validate that the security plan describes the system hardware and its function.

ADVISORY NOTE: The system hardware description includes an equipment list, drawings and diagrams to amplify the description. If the development effort involves a change to existing hardware, identify the specific hardware components being changed. Identify the source of the system hardware, either COTS or government off-the-shelf (GOTS), and provide evaluation and validation-related information, if available. Product evaluation programs include the NIST Cryptographic Module Validation Program (FIPS 140-2), the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Program (ISO/IEC 15408), or other assessment programs approved by the U.S. Government.

REFERENCE: [NIST Special Publication 800-18]

SUBTASK 3.5: Validate that the security plan describes the system firmware and its function.

ADVISORY NOTE: The system firmware description includes, for example, programmable read-only memory (PROM), enhanced PROM (EPROM) devices, or flash RAM devices. Identify the source of the firmware, either COTS or government off-the-shelf (GOTS), and provide evaluation and validation-related information, if available. Product evaluation programs include the NIST Cryptographic Module Validation Program (FIPS 140-2), the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Program (ISO/IEC 15408), or other assessment programs approved by the U.S. Government.

REFERENCE: [NIST Special Publication 800-18]

SUBTASK 3.6: Validate that the security plan describes the system software, (i.e., operating system, middleware, database management system, and security software), and software applications supported by the system and how they will be used.

ADVISORY NOTE: The software description includes manufacturer supplied software and all program generated application software. Identify the source of the system and applications software, either COTS or government off-the-shelf (GOTS), and provide evaluation and validation-related information, if available. Product evaluation programs include the NIST Cryptographic Module Validation Program (FIPS 140-2), the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Program (ISO/IEC 15408), or other assessment programs approved by the U.S. Government.

REFERENCE: [NIST Special Publication 800-18]

SUBTASK 3.7: Validate that the security plan describes the external interfaces to the system including the purpose of each external interface and the relationship between the interface and the system.

REFERENCE: [NIST Special Publication 800-18]

SUBTASK 3.8: Validate that the security plan describes the internal interfaces to the system, data flows including the types of data, general methods for data transmission, and transmission media or interfaces to other systems.

ADVISORY NOTE: The description includes diagrams or text to explain the flow of critical information from one component to another.

REFERENCE: [NIST Special Publication 800-18]

SUBTASK 3.9: Validate that the security plan describes the physical environment in which the system operates including floor plans, equipment placement, electrical and plumbing outlets, telephone outlets, air conditioning vents, sprinkler systems, fences, extension of walls from true floor to true ceiling, alarm systems, guards, etc.

REFERENCE: [NIST Special Publication 800-18]

SUBTASK 3.10: Validate that the security plan lists the number and type of personnel required to operate and maintain the IT system.

REFERENCE: [NIST Special Publication 800-18]

SYSTEM INTERCONNECTION AND INFORMATION SHARING

SUBTASK 3.11: Validate that the security plan lists interconnected systems and unique system identifiers (if appropriate).

REFERENCE: [NIST Special Publication 800-18]

SUBTASK 3.12: Validate that the security plan describes the significant features of the communications layout, including a high level diagram of the communications links and encryption techniques connecting the components of the system, associated data communications, and networks.

REFERENCE: [NIST Special Publication 800-18]

SUBTASK 3.13: Validate that the security plan describes the network connection rules for the system when connected to other (external) systems.

ADVISORY NOTE: After identifying the accreditation boundary, all connections to systems outside that boundary are identified. The purpose of the external connection(s) and the relationship between the connected systems are also documented. Agencies may have additional security requirements for external systems connecting to their systems. These security requirements and those of other systems that may be connected to the system are added to the system security plan and evaluated during the system certification process. C&A documentation is obtained from these external systems to determine the risks of connecting to these systems. Written authorization, (i.e., MOU/MOA and Interconnection Security Agreements) should be obtained prior to connection with other systems and/or sharing sensitive information.

REFERENCE: [NIST Special Publications 800-18, 800-47]

SUBTASK 3.14: Validate that the security plan describes, if applicable, the significant features of web protocols and distributed collaborative computing environments to include: (1) the security controls on web servers and clients, (2) the use of mobile code and/or executable content, (3) any collaborative computing processes or applications, and any distributed processing employed by the system.

REFERENCE: [NIST Special Publication 800-18]

SUBTASK 3.15: Validate that the security plan describes, if applicable, any wireless (RF or IR) devices used in the system.

REFERENCE: [NIST Special Publication 800-18]

SUBTASK 3.16: Validate that the security plan describes, if applicable, the use of Public Key Infrastructure (PKI) and identifies all Certificate Authorities and Certificate Practice Statements.

REFERENCE: [NIST Special Publication 800-18]

APPLICABLE LAWS, REGULATIONS, STANDARDS OR POLICIES AFFECTING THE SYSTEM

SUBTASK 3.17: Validate that the security plan lists any applicable laws, regulations, instructions, directives, standards, or policies that establish specific security requirements for confidentiality, integrity, and availability of information in the system as well as the accountability of those individuals using the system.

ADVISORY NOTE: National level directives, OMB Circulars (A-123 and A-130), general agency directives, agency component level directives, policies, and requirements do not have to be listed since they mandate security for all systems. List only those that are specific to the IT system.

REFERENCE: [NIST Special Publication 800-18]

TASK 4: INITIAL RISK ASSESSMENT

The objective of this task is to validate that the initial risk assessment includes an identification of the threats to and vulnerabilities in the IT system. The initial risk assessment is not performed in lieu of a formal vulnerability analysis, but provides input to a more thorough vulnerability analysis performed later during the certification phase.

THREAT IDENTIFICATION

SUBTASK 4.1: Validate that the initial risk assessment identifies and lists the potential threat-sources that could exploit system vulnerabilities and affect the confidentiality, integrity, and availability of the system.

ADVISORY NOTE: In assessing threat, it is important to consider all potential threat-sources that could cause harm to a system and its processing environment. Threats can be natural, (floods, earthquakes, tornadoes, landslides, avalanches, electrical storms), human, (events that are either enabled by or caused by human beings), or environmental, (long-term power failures, pollution, chemicals, liquid leakage). It should be noted that not all possible threats that might be encountered in the environment need to be listed, only those that are relevant for secure system operation.

REFERENCE: [NIST Special Publication 800-30]

VULNERABILITY IDENTIFICATION

SUBTASK 4.2: Validate that the initial risk assessment identifies and lists system vulnerabilities, (i.e., flaws or weaknesses), that could be exploited by potential threat-sources.

ADVISORY NOTE: Vulnerability source identification can be conducted at any phase in the system development life cycle. If the system has not yet been designed, the search for vulnerabilities should focus on the organization's security policies, planned security procedures, and system requirement definitions, and the developers' security product analyses. If the system is being implemented, the identification of vulnerabilities should be expanded to include more specific information, such as the planned security features described in the security design documentation and the results of the developmental ST&E. If the system is operational, the process of identifying vulnerabilities should include an analysis of the system security controls (management, operational, and technical) used to protect the system. During the initial risk assessment, system vulnerabilities can be identified through the use of vulnerability sources described in NIST Special Publication 800-30. In a subse-

quent phase of the C&A process, (i.e., certification phase) more extensive ST&E activities are employed to uncover additional system vulnerabilities.

REFERENCE: [NIST Special Publication 800-30]

TASK 5: SECURITY CONTROL VALIDATION AND IDENTIFICATION

The objective of this task is to: (1) validate that the security plan describes the security controls for the IT system, and (2) identify any additional security controls not contained in the security plan. The security controls selection is based on the initial characterization of the system from the security plan and any additional controls selected or created based on the initial risk assessment.

SECURITY CONTROL VALIDATION

SUBTASK 5.1: Validate that the security plan contains the necessary security controls for the IT system, (i.e., management, operational, and technical controls) based on the system characterization (obtained from the security plan) expressed as levels of concern (low, moderate, or high), for confidentiality, integrity, and availability; update the security plan as necessary.

ADVISORY NOTE: Minimum-security controls for federal IT systems are listed in NIST Special Publication 800-53. There is a pre-defined standard package of security controls and a supplemental package of controls that can be created by the agency. The standard package includes basic-level security controls for confidentiality, integrity, and availability. This is the baseline set of security controls that should be implemented in all federal systems. The supplemental package allows agencies to increase the level of assurance for their respective IT systems by selecting additional security controls, when needed. The supplemental package corresponds to the increased levels of concern expressed by the agency in the areas of confidentiality, integrity, and availability. Minimum security controls may be augmented with additional controls as needed, in accordance with agency policy and security requirements. To summarize the control validation and identification process for the IT system:

- Validate that the security plan contains the minimum security controls from the standard package of basic controls (mandatory for all systems). [NIST Special Publication 800-53]
- Identify any additional minimum security controls (moderate/high levels), if appropriate, to create a supplemental package of controls based on increased levels of concern for confidentiality, integrity, and/or availability. [NIST Special Publication 800-53]
- Create any additional agency-specific or technology-driven security controls, [if needed security controls are not available in NIST Special Publication 800-53].
- Adjust the selected controls based on internal/external exposure and risk based decisions; describe the controls in documented, allowable waivers.

REFERENCES: [NIST Special Publications 800-18, 800-30, 800-53]

LIST OF ADDITIONAL CONTROLS

SUBTASK 5.2: Construct a *control identification list* for all of the security controls that should be added to the security plan and implemented based on the criticality/sensitivity needs identified earlier. These additional controls should be discussed during the final negotiations (Task 6).

ADVISORY NOTE: The C&A process defines the assessment activities necessary to verify that the security controls have been correctly implemented and are effective. The identification and correct and effective implementation of security controls is a necessary condition to demonstrate compliance with the system security requirements.

REFERENCES: [NIST Special Publication 800-37]

TASK 6: NEGOTIATION

The objective of this task is to validate the information obtained during the pre-certification phase and to conduct a final negotiation with all prospective participants in the C&A process prior to

moving into the actual certification phase. The negotiation provides an opportunity for the DAA, program manager, system owner, information owner, system security officer, and certifier to review the extent and scope of the planned C&A activities and to reach final agreement on the levels of concern for confidentiality, integrity, and availability, the level of concern for system exposure, the certification level, security controls, residual risk, and how the remaining C&A effort will be conducted.

SUBTASK 6.1: Conduct a final negotiation with all participants in the C&A process to agree on scope, activities, and schedule.

REFERENCES: [NIST Special Publications 800-37]

4.2 Certification Phase

The purpose of the certification phase is to demonstrate through independent assessments using selected verification techniques and verification procedures, that the security controls for the IT system have been implemented correctly and are effective in their application. Correct and effective implementation of security controls is a necessary condition to demonstrate compliance with the system security requirements. The results of the certification phase are documented in the developmental and/or operational ST&E reports which are included in the final certification package along with the security plan and final risk assessment report. The certification phase consists of two tasks:

- Verification Procedure Refinement; and
- Security Test and Evaluation (ST&E).

The tasks in the certification phase are appropriate for new systems, major and minor system upgrades, and legacy systems. NIST Special Publication 800-53A (projected for Spring 2003) distinguishes between developmental and operational ST&E activities in the specific verification procedures provided for the security controls. Each verification procedure may have a developmental ST&E component and an operational ST&E component. Typically, the difference in the developmental and operational verification procedures is in the amount of information available at that particular stage in the system development life cycle. For developmental ST&E, there are numerous assumptions made about the environment where the system will operate which cannot be fully verified until the system is deployed for operation. Upon completion of the certification phase, the C&A process proceeds with the accreditation phase. The following sections contain descriptions of all certification tasks and associated subtasks.

TASK 7: VERIFICATION PROCEDURE REFINEMENT

The objective of this task is to develop, where needed, appropriate refinements to the verification procedures associated with the security controls in the standard and supplemental packages to create system-specific technical and non-technical tests. NIST Special Publication 800-53 (projected for Spring 2003) provides recommended verification techniques and generalized verification procedures for all security controls. These techniques and procedures provide guidance to certifiers on the degree of rigor to be applied in the verification process (targeted to the selected SCL) and the specific steps needed to demonstrate that the security controls are implemented correctly and are effective in their application. The *verification procedure refinements*, however, tailor the verification procedures to the specific system and environment where the system is deployed for operation (or in the case of new systems, where the system is intended to be deployed for operation). Verification procedure refinements are only created when the original verification procedures for the security controls (outlined in Special Publication 800-53) do not provide suffi-

cient system-specific information for the certifier to adequately demonstrate that the controls are correctly implemented and effective.

SUBTASK 7.1: Develop, if needed, appropriate refinements to the verification procedures associated with the basic security controls in the standard package and any additional controls in the agency-defined supplemental package (if applicable).

ADVISORY NOTE: Refinements of verification procedures may be necessary to develop specific ST&E activities for particular systems, platforms and/or operational environments. For example, checking the implementation of a password identification and authentication mechanism may require specific information about the system being certified and accredited, (i.e., Windows-based system versus Unix-based system). The verification technique, verification procedure, and procedure refinement provide the certifier with the essential information to effectively carry out the appropriate ST&E activities at the selected SCL.

REFERENCES: [NIST Special Publication 800-53]

TASK 8: SECURITY TEST AND EVALUATION (ST&E)

The objective of this task is: (1) to demonstrate through appropriate verification techniques, verification procedures, and procedure refinements (as needed), that the management, operational, and technical security controls for the IT system are implemented correctly and are effective in their application, and (2) to prepare the final ST&E report(s) based on the results of the ST&E activities carried out during the certification phase.

SCL-1

SUBTASK 8.1a: Demonstrate, through an independent assessment using appropriate **SCL-1** verification techniques and verification procedures (with procedure refinements as needed), that the basic security controls in the standard package and any additional controls in the agency-defined supplemental package **(if applicable)** are implemented correctly and are effective in their application.

SCL-2

SUBTASK 8.1b: Demonstrate, through an independent assessment using appropriate **SCL-2** verification techniques and verification procedures (with procedure refinements as needed), that the basic security controls in the standard package and any additional controls in the agency-defined supplemental package are implemented correctly and are effective in their application.

SCL-3

SUBTASK 8.1c: Demonstrate, through an independent assessment using appropriate **SCL-3** verification techniques and verification procedures (with procedure refinements as needed), that the basic security controls in the standard package and any additional controls in the agency-defined supplemental package are implemented correctly and are effective in their application.

ADVISORY NOTE: Specific **SCL-1**, **SCL-2**, and **SCL-3** verification techniques, (e.g., review, observe, interview, examine, demonstrate, exercise, test, analyze, etc), and verification procedures for the security controls in the *risk management, system development and acquisition, configuration management, system interconnection, personnel security, media protection, physical and environmental protection, contingency planning, incident response capability, hardware and system software maintenance, system and data integrity, security awareness, training, and education, documentation, identification and authentication, logical access, audit,* and *communications* families are provided in NIST Special Publication 800-53. Agencies that have augmented the minimum security controls in the standard and/or supplemental packages, should use the agency-defined verification techniques and verification procedures prepared in Task 5 to demonstrate that the additional controls are implemented correctly and are effective.

REFERENCES: [NIST Special Publication 800-37, 800-53]

SUBTASK 8.2: Prepare the final ST&E report(s).

ADVISORY NOTE: The format for the final ST&E report is defined by the agency. The report, however, must clearly show the results of applying the verification procedures and procedure refinements to the security controls for the IT system. In addition to stating which controls are implemented correctly and are effective in their application, the ST&E report identifies which security controls are only partially implemented, are implemented incorrectly, or are ineffective. The final ST&E report is a key input to the final risk assessment.

REFERENCES: [NIST Special Publications 800-37, 800-53]

4.3 Accreditation Phase

The purpose of the accreditation phase is to complete the final risk assessment on the IT system, update the security plan, prepare the certification findings, and issue the accreditation decision. The final risk assessment takes into account the ST&E results from the certification phase in determining the residual risk for the system after a thorough and impartial assessment of the correctness and effectiveness of the security controls. The certification findings bring together, in the final certification package, all of the relevant information supporting the certification process including the updated security plan, the ST&E report(s), the final risk assessment report, and the certifier's statement. The certification package contains the principal evidence that the DAA uses to make an informed, risk-based decision on whether to fully accredit, partially accredit, or not accredit the IT system for operation. The accreditation phase consists of four tasks:

- Final Risk Assessment;
- Security Plan Update;
- Certification Findings; and
- Accreditation Decision.

Upon completion of the accreditation phase, the C&A process moves into its final phase, the post-accreditation phase. The following sections contain descriptions of all accreditation tasks and associated subtasks.

TASK 9: FINAL RISK ASSESSMENT

The objective of this task is to determine the residual risk to the IT system based on the results of the ST&E activities conducted during the certification phase. The ST&E activities, through a series of verification techniques and verification procedures, demonstrated which of the needed security controls for the system are correctly implemented and are effective in their application, and which controls are not implemented correctly and/or are ineffective. Partial implementation and/or missing security controls are also identified during the certification phase. The residual risk, which is documented in the final risk assessment report, describes the risk remaining for the system after appropriate risk mitigation has occurred, (i.e., security controls implemented, assessed, and corrective actions initiated). The degree of acceptable residual risk is determined by the DAA (with inputs from the program manager or system/data owner) in accordance with the agency's mission requirements.

SUBTASK 9.1: Determine the residual risk to the IT system.

REFERENCES: [NIST Special Publications 800-18, 800-30, 800-37, 800-53]

TASK 10: SECURITY PLAN UPDATE

The objective of this task is to ensure the security plan is updated based on the results of the ST&E activities and the final risk assessment.

SUBTASK 10.1: Update the security plan.

REFERENCES: [NIST Special Publications 800-18, 800-37]

TASK 11: CERTIFICATION FINDINGS

The objective of this task is to prepare the final certification findings and to assemble the final certification package for the DAA. The certification package, prepared by the certifier, includes an updated security plan, developmental and/or operational ST&E reports, final risk assessment report, and certifier's statement. The certification findings represent the collective judgment of the certifier and the certification team in assessing the technical correctness and operational effectiveness of the security controls deemed necessary for the IT system. This independent technical and non-technical assessment is intended to provide the DAA with the most complete information possible regarding the state of the management, operational, and technical controls for the IT system. The certification findings also recommend to the DAA the possible implementation of additional risk mitigation actions that would mitigate the residual risks identified as a result of the ST&E.

SUBTASK 11.1: Prepare the final certification findings and assemble the final certification package.

ADVISORY NOTE: The certification findings, through the certifier's statement and backup documentation, provide the DAA with important information necessary to make an informed, risk-based decision regarding the operation of the IT system. The certification phase is narrowly focused on conducting appropriate ST&E activities with the express purpose of demonstrating, through selected verification techniques and verification procedures that necessary security controls are implemented correctly and are effective in their application. The certifier's statement reflects the state of the security controls, based on the results of the ST&E activities conducted by the certifier and the certification team.

REFERENCES: [NIST Special Publications 800-18, 800-37]

TASK 12: ACCREDITATION DECISION

The objective of this task is for the DAA to review the evidence brought forward in the certification package, (i.e., security plan, ST&E report(s), final risk assessment report, and certifier's statement), and to issue the final accreditation decision for the IT system. This evidence represents the best independent assessment of the correctness and effectiveness of the management, operational, and technical security controls employed to protect the IT system in its operational environment. The accreditation decision takes into account the state of the security controls for the system and the mission requirements of the agency. After employing the necessary security controls, assessing the correctness and effectiveness of those controls, mitigating any unacceptable risks, the level of risk remaining (residual risk) for the system in performing its operational mission must be within tolerable limits as established by the DAA.

SUBTASK 12.1: Review the certification package and issue the final accreditation decision.

ADVISORY NOTE: Based on the information available in the final *certification package*, (i.e., security plan, developmental and/or operational ST&E reports, final risk assessment report, and certifier's statement), the DAA can make a risk-based decision to: (1) grant system accreditation, (2) grant an interim approval to operate the system, or (3) deny system accreditation because the risks to the system are not at an acceptable level. For full accreditation, no restrictions apply. For interim accreditation, the system does not meet the security requirements defined in the security plan and does not employ the necessary se-

curity controls to fully protect the information being processed, stored, or transmitted. Mission criticality, however, mandates the system become operational and no other capability exists to adequately perform the mission. Interim accreditation is a temporary approval issued for the minimal period of time necessary to meet the system security requirements and to implement the necessary security controls outlined in the security plan. For accreditation disapproval, the system does not meet the security requirements stated in the security plan and the requisite security controls are either not present or largely ineffective. Accepted risk is too great and mission criticality does not mandate the immediate operational need. The accreditation decision is documented in the final *accreditation package*, which consists of the accreditation letter and supporting documentation and rationale for the accreditation decision. In some situations, IT systems may involve multiple DAAs. If so, agreements must be established among the responsible DAAs and the agreements should be documented in the accreditation package. In most cases, it is advantageous to agree to a lead DAA who represents the other DAAs during the C&A process.

REFERENCES: [NIST Special Publications 800-18, 800-37]

SUBTASK 12.2: For interim accreditations, implement operational restrictions and issue interim accreditation action plan.

ADVISORY NOTE: When systems must be operated due to mission criticality with security deficiencies, (i.e., security controls not correctly implemented, ineffective, or missing), operational restrictions are imposed. Countermeasures (specific protections) can be added but are usually limited to procedural or physical measures. It is not practical or cost-effective under normal circumstances to add internal technical controls late in the system life cycle. Selected system features causing major problems or creating high risk can be removed or their implementation delayed. The number of users or user privileges can also be restricted. Remote terminals can be physically or logically disconnected when sensitive (unclassified) or national security (classified) information is processed or stored. Noted restrictions are documented in an *interim accreditation action plan*. An interim accreditation action plan is created for the IT system and is issued to the program manager or system owner by the DAA along with the interim accreditation letter. The action plan includes: (1) the critical mission that mandates the system be operational, (2) the list of specific corrective actions necessary to demonstrate the needed security controls are implemented correctly and are effective, (3) the agreed upon timeline for taking designated corrective actions, (4) the resources necessary to properly complete the corrective actions, and (5) operational restrictions that are imposed to lessen the risk during the interim accreditation.

REFERENCES: [NIST Special Publications 800-18, 800-37]

4.4 Post-Accreditation Phase

The purpose of the post-accreditation phase is to monitor the status of the IT system to determine if there are any significant changes to the system configuration, (i.e., modifications to the system hardware, software, or firmware), or to the operational/threat environment that might effect the confidentiality, integrity, and/or availability of the information processed, stored, or transmitted by the system. The monitoring activity is necessary to ensure an acceptable level of residual risk is preserved for the system. When changes to the system or to the system's operational/threat environment are deemed significant to the security of the IT system, reaccreditation activities are initiated. Reaccreditation requirements may vary from agency to agency and be either time-driven or event-driven. Refer to applicable laws, regulations, directives, and/or policies to obtain guidance on reaccreditation requirements. The post-accreditation phase consists of three tasks:

- Risk Assessment Update;
- System and Environment Update;
- Reaccreditation; and

- System Disposal.

The post-accreditation phase is a continuous process that is necessary to address the dynamic nature of agency missions and the rapidly changing technologies employed by agencies to support those missions.. The following sections contain descriptions of all post-accreditation tasks and associated subtasks.

TASK 13: RISK ASSESSMENT UPDATE

The objective of this task is to continuously monitor and review open source and other available threat and vulnerability information to assess the potential impact of new threats and vulnerabilities on the IT system and its operational environment. The newly identified threats and vulnerabilities may necessitate a review of: (1) the levels of concern for confidentiality, integrity, availability, and system exposure, (2) the security controls, and (3) the certification level, to ensure the system remains adequately protected.

SUBTASK 13.1: Monitor applicable sources for new threats and vulnerabilities that apply to the accredited IT system and/or its operational environment.

ADVISORY NOTE: New threats and vulnerabilities may impact the accredited IT system security controls. The controls may require adjustment, update, strengthening, or redesign. There are numerous public (open) sources for threat, vulnerability, and countermeasure information. These sources provide checklists, system administration tips, detailed information on specific threats, vulnerabilities, and countermeasures, and security tools.

REFERENCES: [NIST Special Publications 800-18, 800-30, 800-37]

SUBTASK 13.2: Update the risk assessment report, as needed.

REFERENCES: [NIST Special Publications 800-18, 800-30, 800-37]

TASK 14: SYSTEM AND ENVIRONMENT UPDATE

The objective of this task is to carefully track all modifications to the IT system or its supporting operational environment. The DAA, program manager, and system owner must be vigilant in maintaining the security posture of the system. Changes to the system may affect the way security controls work or may create new vulnerabilities. Likewise, the environment provides a certain amount of security protection to the system and must be continuously monitored for changes that might affect the security posture of the system. Strong configuration management practices ensure that all system modifications are documented—the first step in assessing the potential impact of those changes to the security of the system. Continuous improvements to the system must be able to occur without necessarily triggering the reaccreditation process. To accomplish this type of controlled change, each modification, proposed or actual, is assessed for its potential impact on the security of the system. After the system modification is completed and it is verified that the change does not affect the security of the system, the security plan is appropriately updated. If the security of the system is affected, a reaccreditation may be initiated.

SUBTASK 14.1: Review all modifications to the IT system or the system's operational environment to determine the potential security impacts of those modifications.

ADVISORY NOTE: Any proposed modifications to an accredited system or its environment might invalidate the original system accreditation. Having a configuration management or change control process in place reduces the possibility that modifications to the system or environment, (e.g., facility) may compromise the system's confidentiality, integrity or availability. The configuration management process assists in maintaining the system security baseline, controlling and monitoring changes to the system, and identifying when selected changes necessitate recertification or reaccreditation. Where necessary, modification re-

quests are disapproved until appropriate security-relevant changes are made. When changes are made to an accredited system, determine the best way to implement the new hardware, firmware, or software to assure the confidentiality, integrity and/or availability of the system. Where necessary, a transition plan is developed to securely migrate the system over time.

SUBTASK 14.2: Update the security plan, as needed.

REFERENCES: [NIST Special Publications 800-18, 800-37]

TASK 15: REACCREDITATION

The objective of this task is to identify significant changes to the IT system or its surrounding operational environment that necessitate reaccreditation. The DAA, in consultation with the program manager or system owner, determines the conditions under which the system must be reaccredited. Reaccreditation can be either event-driven or time-driven depending on the laws, regulations, directives, instructions, or policies which dictate such activity. For example, OMB Circular A-130 requires reaccreditation every three years or whenever significant changes occur to a system; some agencies may require reaccreditation yearly. In any case, the reaccreditation of the system begins with the pre-certification phase and consists of all tasks completed during the original C&A process. Depending on the nature and extent of the modifications to the system and its supporting environment, a significant portion of the original certification documentation and ST&E results may still be applicable. Reuse of previous certification evidence is an effective method of reducing assessment costs during the reaccreditation process.

SUBTASK 15.1: Determine the need for reaccreditation of the IT system.

ADVISORY NOTE: There are many variables that may necessitate reaccreditation of the IT system. The most common reason for reaccrediting the system is a change in the system/environment baseline that impacts security. The reaccreditation efforts then concentrate on those changes since the original accreditation. The following is a partial list of events affecting security that may require a system to be reaccredited: (1) changes to levels of concern for confidentiality, integrity and/or availability, (2) hardware, software, or firmware additions, modifications, or upgrades requiring changes in the approved security controls, (3) threat changes creating system vulnerabilities resulting in higher risk, (4) mission changes, (5) breaches of security, breaches of system integrity, or unusual situations that appear to invalidate the accreditation by revealing flaws in security design exposing vulnerabilities, (6) significant changes in the physical structure of the facility, (7) significant changes in operating procedures, (8) system configuration changes, (9) the inclusion of additional separately accredited systems, and (10) the results of an audit or external analysis. When the need for reaccreditation is identified, revert to the pre-certification phase.

REFERENCES: [NIST Special Publication 800-37]

TASK 16: SYSTEM DISPOSAL

The objective of this task is to ensure that an IT system reaching the end of its life cycle, and having been identified for disposal, is taken out of the operational environment and disposed of in a secure manner. There are three important areas of concern that must be addressed when a system has been identified for elimination: (1) the archival of information, (2) the disposal of hardware, firmware, and software, and (3) the sanitization of media.

SUBTASK 16.1: Dispose of the IT system in a secure manner in accordance with agency policies and procedures.

ADVISORY NOTE: Usually there is no definitive end to a system life cycle. Systems evolve or transition to the next generation as a result of changing requirements or improvements in technology. Security plans should continually evolve with the system. Even in situations where a system is identified to cease operation (e.g., AUTODIN to DMS transition), if the

security plan was kept updated much of the environmental, management, and operational information should still have relevance and be useful in developing the security plan for the follow-on system.

Information Archival. When archiving information, agencies should consider additional methods for retrieving information in the future. While electronic information is easier to retrieve and store, the technology used to create the records may not be readily available in the future. Legal requirements for records retention should also be considered when disposing of IT systems.

Hardware, Firmware, and Software. Hardware, firmware, and software can be sold, given away, or discarded. There is rarely a need to destroy hardware, except for some storage media containing classified information that cannot be sanitized without destruction. The disposition of software should comply with license or other agreements with the developer.

Media Sanitization. The removal of information from a storage medium is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information and purging information. Clearing information is removal of sensitive data from a storage device at the end of a processing period in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed using normal system capabilities (e.g., through the keyboard). Purging is the removal of data from a storage device at the end of a processing period in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed through open-ended laboratory techniques. Degaussing, overwriting, and media destruction are some of the methods to purge information. Degaussing is a process whereby the magnetic media is erased. Overwriting is a process whereby unclassified data is written to storage locations previously containing sensitive data. Media may be destroyed by: (1) destruction at an approved metal destruction facility (e.g., smelting, disintegration, or pulverization), (2) incineration, or (3) application of an abrasive substance to a magnetic disk.

REFERENCES: [NIST Special Publication 800-37]

ANNEX A

REFERENCES

LAWS, POLICIES, REGULATIONS, STANDARDS, AND SPECIAL PUBLICATIONS

1. FY2001 Defense Authorization Act (P.L. 106-398) including Title X, Subtitle G, *Government Information Security Reform*.
2. Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, February 1996.
3. NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.
4. *Common Criteria for Information Technology Security Evaluation* (ISO/IEC Standard 15408), Version 2.1, August 1999.
5. Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.
6. NIST Special Publication 800-16, *IT Security Training Requirements: A Role and Performance-Based Model*, April 1998.
7. NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.
8. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, October 2001.
9. Presidential Decision Directive 63, *Protecting America's Critical Infrastructures*, May 1998.
10. General Accounting Office *Federal Information System Control Audit Manual* (FISCAM), January 1999.
11. NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Security Information Technology Systems*, September 1996.
12. Special Publication 800-53, *Minimum Security Controls for Federal Information Technology Systems* (projected for Spring 2003).
13. Special Publication 800-53A, *Techniques and Procedures for the Verification of Security Controls in Federal Information Technology Systems* (projected for Spring 2003).
14. Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.
15. Special Publication 800-14, *Generally Accepted Principles and Practices for Security Information Technology Systems*, September 1996.
16. Health Care Information Portability and Accountability Act of 1996 (HIPAA)
17. The Privacy Act of 1974.
18. NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

This page left intentionally blank.

ANNEX B

GLOSSARY

COMMON TERMS FOR THE CERTIFICATION AND ACCREDITATION PROCESS

Acceptable Risk	A concern that is acceptable to responsible management, due to the cost and magnitude of implementing security controls.
Accountability	Property that allows the ability to identify, verify, and trace system entities as well as changes in their status. Accountability is considered to include authenticity and non-repudiation.
Accreditation	The authorization of an IT system to process, store, or transmit information, granted by a management official. Accreditation, which is required under OMB Circular A-130, is based on an assessment of the management, operational, and technical controls associated with an IT system.
Accreditation Disapproval	The system does not meet the security requirements and security controls as stated in the security plan; residual risk is too great, and mission criticality does not mandate the immediate operational need. Therefore, the developmental system is not approved for operation or, if the system is already operational, the operation of the system is halted.
Accreditation Package	The accreditation letter and supporting documentation and rationale for the accreditation decision.
Accreditation Phase	The accreditation phase is the third phase of the certification and accreditation process. Its purpose is to complete the final risk assessment on the IT system, update the security plan, prepare the certification findings, and issue the accreditation decision.
Adequate Security	Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Audit	A family of security controls in the technical class dealing with ensuring activity involving access to and modification of sensitive or critical files is logged, monitored, and possible security violations investigated.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Authorize Processing	Occurs when management authorizes a system based on an assessment of management, operational and technical controls. By authorizing processing in a system the management official accepts the risk associated with it.
Availability	Assurance that information, services, and IT system resources are accessible to authorized users and/or system-related processes on a timely and reliable basis and are protected from denial of service.

Certification	The comprehensive evaluation of the technical and non-technical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.
Certification Agent or Certifier	The individual (and supporting team) responsible for making an independent technical and non-technical evaluation of a system based on the security requirements and security controls documented in the security plan. The certifier assesses the vulnerabilities in the system, determines if the security controls are correctly implemented and effective, and identifies the level of residual risk.
Certification Level	See security certification level.
Certification Package	Product of the certification effort documenting the detailed results of the certification activities. The certification package includes the security plan, developmental and/or operational ST&E reports, risk assessment report, and certifier's statement.
Certification Phase	The certification phase is the second phase of the certification and accreditation process. Its purpose is to demonstrate through independent assessments using selected verification techniques and verification procedures that the security controls for the IT system have been implemented correctly and are effective in their application.
Clearance	The official determination of a person's trustworthiness, based on a records review and past behavior.
Communications	A family of security controls in the technical class dealing with ensuring that communications are appropriately protected by encryption or PDSs, that controlled interfaces are installed and appropriately configured as required to protect the IT system, and that dial-in and remote access is appropriately controlled, protected, and monitored.
Component	An IT assembly, or part thereof, that is essential to the operation of some larger IT assembly and is an immediate subdivision of the IT assembly to which it belongs, (e.g., a trusted guard, biometrics device, or firewall would be a component of a computer system.).
Confidentiality	Assurance that information in an IT system is not disclosed to unauthorized persons, processes or devices.
Configuration Management	A family of security controls in the management class dealing with the control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an IT system.
Contingency Planning	A family of security controls in the operations class dealing with emergency response, backup operations, and post-disaster recovery for an IT system, to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

Control Class	A grouping of security controls, organized by control families, that all fall under the same broad category. For example, there are three general classes of security controls, (i.e., management, operational, and technical) in NIST Special Publications 800-18, 800-37, and 800-53.
Control Family	A grouping of security controls that fall under the same more specific category, which are often interrelated and interdependent, and which should be considered as a group.
Control Identification List	A list of all of the security controls that should be added to the security plan and implemented based on the criticality/sensitivity needs identified by the agency.
Countermeasure	See security control.
Critical Elements	Important security-related focus areas for the system with each critical element addressed by one or more security controls.
Criticality/sensitivity	A measure of the importance and nature of the information processed, stored, and transmitted by the IT system to the organization's mission and day-to-day operations.
Data Integrity	Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered or destroyed.
Defense-In-Depth	A two-fold approach to securing an IT system: (1) layering security controls within a given IT asset and among assets, and (2) ensuring appropriate robustness of the solution as determined by the relative strength of the security controls and the confidence that the controls are implemented correctly, are effective in their application, and will perform as intended. This combination produces layers of technical and non-technical controls that ensures the confidentiality, integrity, and availability of the information and IT system resources.
Designated Approving Authority (DAA)	Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.
Developer	The organization or individual that develops the IT system.
Documentation	A family of security controls in the operations class dealing with the documentation it is necessary to maintain for the secure operation of an IT system. Documentation can include contingency plans, user manuals, hardware, software and application manuals, etc.
Entry-level Certification	The most basic certification level, appropriate for systems engendering low levels of concern for confidentiality, integrity, and availability.
Environment	Aggregate of external procedures, conditions, and objects affecting the development, operation and maintenance of an IT system.
Exposure	A measure of the potential risk to an IT system from both external and internal threats.

External System Exposure	Relates to: (1) the method by which users access the system, (e.g., dedicated connection, intranet connection, Internet connection, wireless network), (2) the existence of backend connections to the system and to what the backend systems are connected, and (3) the number of users that access the system.
Facility Manager	Oversees changes and additions to the facility housing the IT system and ensures changes in facility design or construction do not adversely affect the security of existing systems.
Firmware	Program recorded in permanent or semi permanent computer memory.
Full accreditation	The system security requirements have been satisfied and the security controls have been implemented correctly and are operating effectively. The system is approved to operate in the intended environment as stated in the security plan and few, if any, restrictions on processing apply.
General Support System	An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people, and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.
Hardware and System Software Maintenance	A family of security controls in the operations class dealing with the secure maintenance activities of hardware and system software.
Identification and Authentication	A family of security controls in the technical class dealing with ensuring that users are individually authenticated via passwords, tokens, or other devices, and that access controls to the IT system are enforcing segregation of duties.
Incident Response Capability	A family of security controls in the operations class dealing with responding to an assessed occurrence having actual or potentially adverse effects on an IT system.
Independent Assessment	In this document, an evaluation of how well an IT system and its operating environment meet its required security controls, performed by an organization or individual that does not have a vested interest in the outcome of the assessment. An independent assessment can be performed by individuals either internal or external to the agency undergoing the evaluation, as long as they are free from personal and external factors that could impair their independence or their perceived independence, (e.g., they designed the system under review).
Individual Accountability	Requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.
Information System	See IT System.
IT Security	Information operations protect and defend information and IT systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of IT systems by incorporating protection, detection and reaction capabilities.

IT System	The set of agency information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Categories of IT systems are major applications and general support systems.
Integrity	Assurance that information in an IT system is protected from unauthorized, unanticipated, or unintentional modification or destruction. System integrity also addresses the quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.
Interconnection Security Agreements	An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations.
Interim Accreditation	Temporary authorization granted by a DAA for an IT system to process, store and/or transmit information based on preliminary results of security certification of the system.
Interim Accreditation Action Plan	A document created for the IT system which has received an interim accreditation to operate, and which is issued to the program manager or system owner by the DAA along with the interim accreditation letter. The action plan includes: (1) the critical mission that mandates the system be operational, (2) the list of specific corrective actions necessary to demonstrate the needed security controls are implemented correctly and are effective, (3) the agreed upon timeline for taking designated corrective actions, (4) the resources necessary to properly complete the corrective actions, and (5) operational restrictions that are imposed to lessen the risk during the interim accreditation.
Internal System Exposure	Relates to the types of individuals that have authorization to access the system and the information the system stores, processes, and transmits. It includes such items as individual security background assurances and/or clearance levels, access approvals, and need-to-know.
Levels of Concern	An expression of the criticality/sensitivity of an IT system in the areas of confidentiality, integrity, availability, and exposure, expressed qualitatively as high, moderate or low. The level of concern indicates the extent to which security controls must be applied to an IT system based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs.
Logical Access	A family of security controls in the technical class dealing with ensuring that logical access controls on the IT system restrict users to authorized transactions and functions.

Major Application	An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.
Management Controls	Controls that address management of the security aspects of the IT system and the management of risk for the system. Management controls include risk management, review of security controls, system life cycle controls, processing authorization controls, and system security plan controls.
Media Protection	A family of security controls in the operations class dealing with the protection of system inputs and outputs from unauthorized exposure.
Memorandum of Understanding Memorandum of Agreement	A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. An MOU/MOA defines the responsibilities of two or more organizations in establishing, operating and securing a system interconnection.
Mid-level Certification	More stringent than an entry-level certification, this certification level is appropriate for systems engendering moderate levels of concern for confidentiality, integrity, and/or availability.
National Security Information	Information that has been determined pursuant to Executive Order 12958 or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. National security information includes Sensitive Compartmented Information (SCI) concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.
National Security System	IT system operated by the U.S. Government, its contractors, or agents that contains classified information or, as set forth in 10 U.S.C. Section 2315, that involve: intelligence activities or cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapon system, or equipment that is critical to the direct fulfillment of military or intelligence missions.
Need-to-know	The necessity for access to, or knowledge or possession of, specific information required to carry out official duties.
Networks	IT system implemented with a collection of interconnected network nodes.
Non-repudiation	Assurance the sender of data 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 data.
Operational Controls	Controls that address security mechanisms primarily implemented and executed by people (as opposed to systems)

Operations Manager	Oversees the security operations and administration of the IT system to include performing backups, holding training classes, managing cryptographic keys, keeping up with user administration and access privileges, and updating security software.
Personnel Security	A family of security controls in the operations class dealing with background screenings, appropriate access privileges, etc.
Physical and Environmental Protection	A family of security controls in the operations class dealing with the protection of an IT system and its environment from threats related to the facility in which it is housed. Physical and environmental protection procedures include securing the facility perimeter from unauthorized access, to protection from faulty plumbing lines, to protecting against environmental threats such as hurricane or fire.
Post-accreditation Phase	The post-accreditation phase is the last and ongoing phase of the certification and accreditation process. Its purpose is to monitor the status of the IT system to determine if there are any significant changes to the system configuration, (i.e., modifications to the system hardware, software, or firmware), or to the operational/threat environment that might effect the confidentiality, integrity, and/or availability of the information processed, stored, or transmitted by the system. The monitoring activity is necessary to ensure an acceptable level of residual risk is preserved for the system. When changes to the system or to the system's operational/threat environment are deemed significant to the security of the IT system, reaccreditation activities are initiated.
Pre-certification Phase	The pre-certification phase is the first phase of the certification and accreditation process. Its purpose is to prepare for the verification activities that will take place during the certification phase. The pre-certification phase consists of six tasks: system identification; initiation and scope determination; security plan validation; initial risk assessment; security control validation and identification; and negotiation.
Program Manager	The individual responsible for the IT system during initial development and acquisition. The program manager is concerned with cost, schedule, and performance issues for the system as well as security issues.
Residual Risk	Portion of risk remaining after security controls have been applied.
Risk	The net mission impact considering: (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular IT system vulnerability and (2) the resulting impact if this should occur. IT system-related risks arise from legal liability or mission loss due to: (1) unauthorized (malicious or accidental) disclosure, modification, or destruction of information, (2) unintentional errors and omissions, (3) IT disruptions due to natural or man-made disasters, and (4) failure to exercise due care and diligence in the implementation and operation of the IT system.

Risk Assessment	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of risk management and synonymous with risk analysis.
Risk Management (1)	A family of security controls in the management class dealing with the process of identifying and applying controls commensurate with the value of the assets protected based on a risk assessment.
Risk Management (2)	The total process of identifying, controlling, and mitigating IT system-related risks. It includes risk assessment; cost benefit analysis; and the selection, implementation, test and security evaluation of security controls. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.
Rules Of Behavior	The rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment and limitation of system privileges, and individual accountability.
Safeguard	See security control.
Security	See computer security.
Security Awareness, Training, and Education	A family of security controls in the operations class dealing with ensuring that employees receive adequate training to fulfill their security responsibilities.
Security Certification Level	A combination of techniques and procedures used during a C&A process to verify the correctness and effectiveness of security controls in an IT system. Security certification levels, identified as SCL-1, SCL-2, or SCL-3, represent increasing levels of intensity and rigor in the verification process and include such techniques as reviewing and examining documentation, interviewing personnel, conducting demonstrations and exercises, conducting functional, regression, and penetration testing, and analyzing system design documentation.
Security Controls	Management, operational, and technical measures prescribed for an IT system which, taken together, satisfy the specified security requirements and protect the confidentiality, integrity, and availability of the system and its information. Security controls can be selected from a variety of families including risk management, system development and acquisition, configuration management, system interconnection, personnel security, media protection, physical and environmental protection, contingency planning, incident response capability, hardware and system software maintenance, system and data integrity, security awareness, training, and education, documentation, identification and authentication, logical access, audit, and communications.

Security Program Manager	Ensures a standard C&A process is used throughout the agency, provides internal C&A guidance or policy, and, if appropriate, reviews certification packages prior to DAA review.
Security Test & Evaluation (ST&E)	The techniques and procedures employed during a C&A process to verify the correctness and effectiveness of security controls in an IT system. There are typically two types of ST&E activities, (i.e., developmental and operational ST&E), that can be applied during the certification phase depending on where the system is in the system development life cycle.
Sensitive Information	Information the loss, misuse, or unauthorized access to or modification of, which would adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L. 100-235). Some specific categories of sensitive information are protected by statute, regulation or contract, (e.g., privacy information, proprietary information, export control information, pre-publication academic information).
Site Accreditation	An accreditation where all systems at a location are grouped into a single management entity. A DAA may determine that a site accreditation approach is optimal given the number of IT systems, major applications, networks, or unique operational characteristics. Site accreditation begins with all systems and their interoperability and major applications at the site being certified and accredited. The site is then accredited as a single entity, and an accreditation baseline is established.
Subsystem	A major subdivision or component of an IT system consisting of hardware/software/firmware that performs a specific function.
System	A generic term used for briefness to mean either a major application or a general support system.
System Accreditation	Authorizes the operation of a major application or a general support system at a particular location with specified environmental constraints.
System Authorization	See system accreditation.
System and Data Integrity	A family of security controls in the operations class dealing with the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data.
System Boundary	Encompasses all those components of the system that are to be accredited by the DAA and excludes separately accredited systems, to which the system is connected.
System Development and Acquisition	A family of security controls in the management class dealing with the design, development and acquisition of IT systems.

System Interconnection	A family of security controls in the management class dealing with the operational, technical, and management requirements for interconnecting IT systems.
System Owner	Represents the interests of the user community and the IT system throughout the system's life cycle. The system owner assumes responsibility for the system after delivery and installation during operation, maintenance, and disposal.
System Security Officer	The person responsible to the Designated Approving Authority, program manager, and/or system/data owner for ensuring the security of an IT system throughout its life cycle, from design through disposal.
Security Plan	Formal document that provides an overview of the security requirements of the IT system and describes the security controls in place or planned for meeting those requirements.
Technical Controls	Consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the IT system and applications.
Threat	The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability; or Any circumstance or even with the potential to harm an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
Threat Source	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.
Top-level Certification	More stringent than a mid-level certification, this certification level is appropriate for systems engendering high levels of concern for confidentiality, integrity, and/or availability.
Type Accreditation	In some situations, a major application or general support system is intended for installation at multiple locations. The application or system usually consists of a common set of hardware, software, and firmware. Type accreditations are a form of interim accreditation and are used to certify and accredit multiple instances of a major application or general support system for operation at approved locations with the same type of computing environment.
User	Person or process authorized to access an IT system.
User Representative	The individual or organization that represents the operational interests of the user community and serves as the liaison for that community throughout the life cycle of the system. The user representative also assists in the C&A process, when needed, to ensure mission requirements are satisfied while meeting the security requirements defined in the security plan.
Validation	Confirmation, through review and/or examination, that relevant security-related policies, plans, procedures, or documents have been completed and/or any security-related activities accomplished in support of the C&A process.
Verification	The assessment process, including techniques and procedures, used to demonstrate that security controls for an IT system are implemented correctly and are effective in their application.

Verification Procedure Refinements	Verification procedures that have been tailored to the specific system and environment where the system is deployed for operation (or in the case of new systems, where the system is intended to be deployed for operation).
Verification Techniques	Specific approaches that can be employed during the C&A process to demonstrate compliance with the security requirements and to determine the correctness and effectiveness of the security controls.
Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the systems security policy.

This page left intentionally blank.

ANNEX C

ACRONYMS

SHORTHAND NOTATIONS FOR CERTIFICATION AND ACCREDITATION-RELATED TERMS

C&A	Certification and Accreditation
COTS	Commercial Off The Shelf
DAA	Designated Approving Authority
EPROM	Enhanced Programmable Read Only Memory
FIPS	Federal Information Processing Standards
GOTS	Government Off The Shelf
IT	Information Technology
LAN	Local Area Network
MOA	Memorandums of Agreement
MOU	Memorandums of Understanding
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
PROM	Programmable Read Only Memory
SCI	Sensitive Compartmented Information
SCL	Security Certification Level

This page left intentionally blank.

ANNEX D

SAMPLE ACCREDITATION LETTERS

ACCREDITATION, INTERIM ACCREDITATION, AND ACCREDITATION DISAPPROVAL

Sample Certification Package Transmittal Letter

To: Designated Approving Authority Date:
From: Certification Agent
Subject: Security Certification of [IT SYSTEM]

A certification review of the [IT SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] has been conducted in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, and the [ORGANIZATION] Certification and Accreditation Program. The attached certification package transmits the following items: (1) the current security plan for the IT system, (2) the results of the security test and evaluation (ST&E) activities, and (3) the final risk assessment report.

The security controls listed in the security plan for the [IT SYSTEM] have been assessed using the verification techniques and the verification procedures described in the ST&E report to determine if those controls are implemented correctly and are effective in their application, and accordingly, if the security requirements for the system have been satisfied. Based on the results of the ST&E activities, a final risk assessment report has been prepared stating the corrective measures that have been implemented or are planned to mitigate the risks associated with the identified vulnerabilities. The risk assessment report also identifies the remaining residual risks for the [IT SYSTEM] after the risk mitigation activities have been completed.

Signature:

Title:

Accreditation Decision Letter (Full Accreditation)

To: Senior Official Date:
From: Designated Approving Authority
Subject: Security Accreditation of [IT SYSTEM]

A certification review of the [IT SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] has been conducted in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, and the [ORGANIZATION] Certification and Accreditation Program. I have carefully reviewed the results of the security certification and the supporting evidence provided in the certification package, (i.e., the current security plan for the IT system, the results of the security test and evaluation (ST&E) activities, and the final risk assessment report).

EITHER

(1) In accordance with the provisions of the [ORGANIZATION] Certification and Accreditation Program, after reviewing the security controls that have been implemented and planned, and weighing the remaining residual risks against the operational requirements, the [IT SYSTEM] is approved for initial/continued operation at Security Certification Level [1, 2, OR 3]. This authorization is my formal declaration that appropriate system security controls have been properly implemented and that a satisfactory level of security is present.

OR

(2) In accordance with the provisions of the [ORGANIZATION] Certification and Accreditation Program, after reviewing the security controls that have been implemented and planned, and weighing the remaining residual risks against the operational requirements, the [IT SYSTEM] is authorized for initial/continued operation at Security Certification Level [1, 2, OR 3] with the following restrictions:

[DESCRIPTION OF LIMITS TO OPERATION]

This authorization is my formal declaration that under the restrictions listed above, the appropriate system security controls have been properly implemented and that a satisfactory level of security is present.

This authorization is for the existing operating environment of the [IT SYSTEM], is contingent upon continued application of the security controls in place, and is valid for a period of [TIME] from the date of this letter unless a significant change to the IT system requires earlier reaccreditation. It is the responsibility of the senior official in charge of the system to ensure that any significant change in the system's configuration, (i.e., hardware, software, and/or firmware), or the system's operating environment is analyzed to determine its impact on system security and that appropriate action is taken to maintain a level of security consistent with the requirements for this action.

The Systems Security Officer (SSO) should retain a copy of this accreditation letter with all supporting documentation as a permanent record.

Signature:

Title:

Accreditation Decision Letter (Interim Accreditation)

To: Senior Official Date:
From: Designated Approving Authority
Subject: Security Accreditation of [IT SYSTEM]

A certification review of the [IT SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] has been conducted in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, and the [ORGANIZATION] Certification and Accreditation Program. I have carefully reviewed the results of the security certification and the supporting evidence provided in the certification package, (i.e., the current security plan for the IT system, the results of the security test and evaluation (ST&E) activities, and the final risk assessment report).

In accordance with the provisions of the [ORGANIZATION] Certification and Accreditation Program, after reviewing the security controls that have been implemented and planned, and weighing the remaining residual risks against the operational requirements, the [IT SYSTEM] is approved, on an interim basis, for initial/continued operation at Security Certification Level [1, 2, OR 3]. This interim authorization is my formal declaration that some security controls for the [IT SYSTEM] have been properly implemented; however, additional security controls are needed to ensure that a satisfactory level of security is present. The [IT SYSTEM] may be operated in a limited mode (see below) until additional security controls as specified in Attachment A can be implemented. Attachment A also contains the schedule for implementation of the additional security controls.

[DESCRIPTION OF LIMITS TO OPERATION]

The System Security Officer (SSO) will monitor the implementation of the additional security controls and notify the DAA if deviations from the schedule occur. When all additional security controls are implemented and working as proposed, the operating restrictions will be removed. This interim authorization is for the existing operating environment of the [IT SYSTEM], is contingent upon continued application of the security controls in place, and is valid for a period of [TIME] from the date of this letter unless a significant change to the IT system requires earlier reaccreditation. It is the responsibility of the senior official in charge of the system to ensure that any significant change in the system's configuration, (i.e., hardware, software, and/or firmware), or the system's operating environment is analyzed to determine its impact on system security and that appropriate action is taken to maintain a level of security consistent with the requirements for this action.

The Systems Security Officer (SSO) should retain a copy of this accreditation letter with all supporting documentation as a permanent record.

Signature:

Title:

Attachment A

Accreditation Decision Letter (Accreditation Disapproval)

To: Senior Official Date:
From: Designated Approving Authority
Subject: Security Accreditation of [IT SYSTEM]

A certification review of the [IT SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] has been conducted in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, and the [ORGANIZATION] Certification and Accreditation Program. I have carefully reviewed the results of the security certification and the supporting evidence provided in the certification package, (i.e., the current security plan for the IT system, the results of the security test and evaluation (ST&E) activities, and the final risk assessment report).

In accordance with the provisions of the [ORGANIZATION] Certification and Accreditation Program, after reviewing the security controls that have been implemented and planned, and weighing the remaining residual risks against the operational requirements, the [IT SYSTEM] is not approved for initial/continued operation. This disapproval is my formal declaration that the [IT SYSTEM] is lacking appropriate security controls and that the risks resulting from its operation are unacceptable. The attached residual risk statement explains the reasons for denying accreditation. A list of additional security controls is also attached, that if implemented properly, would provide the level of security required for accreditation.

It is the responsibility of the senior official in charge of the [IT SYSTEM] to ensure that system is not placed into operation until the additional security controls as specified, are properly implemented. The senior official will also ensure that the certification team analyzes the implementation of the additional security controls and submits a new certification package for review by the Designated Approving Authority before the system becomes operational.

The Systems Security Officer (SSO) should retain a copy of this accreditation letter with all supporting documentation as a permanent record.

Signature:

Title:

Attachment A