Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Many Facets of an Information Security Program

This document is a review of the various programs and processes that should be in place within any organization for the protection of their information assets. The many areas of any organization's security program play key roles in supporting the certification and accreditation (C&A) process of an organization's information assets. The supporting areas along with the C&A and post C&A activities make up an organization's information security program. Five primary sections herein outline an information security program b...

Copyright SANS Institute
Author Retains Full Rights

AD

The Many Facets of an Information Security Program

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b, Option 1

Robert L Behm, Jr.
06 December 2003

© SANS Institute 2004, Author retains full rights.

Table Of Contents

I. Introduction 1

II. Audience 1

III. The Information Security Program 2

IV. Security Laws & Regulations 2
- A. Federal Information Security Management Act 2
- B. Health Insurance Portability and Accountability Act of 1996 3
- C. Office of Management and Budget Circular A-130 3

V. Security Standards & Best Practices 4
- A. National Institute of Standards and Technology 4
- B. International Organization for Standardization 5
- C. SANS (SysAdmin, Audit, Network, Security) 5
- D. Center for Internet Security 5

VI. Organization's Supporting Programs 6
- A. Security Policies 7
- B. Physical Security 7
- C. Personnel Security 8
- D. System and Data Identification 8
- E. Incident Response Program 9
- F. System Security Plan 10
- G. System Development Life Cycle 11
- H. Configuration Management 12
- I. Training and Awareness Program 12
- J. System Documentation 14
- K. Disaster Recovery 15

VII. Certification and Accreditation (C&A) Program 15
- A. Certification Process 16
- B. Accreditation Process 21
- C. Post Accreditation Activities 22

VIII. Summary 23

Table of Figures

Figure 1 - Overview of an Information Security Program 2
Figure 2 - Organization's Supporting Security Policies & Programs 6
Figure 3 - An Information System's Certification Process 16
Figure 4 - An Information System's Accreditation Process 21
Figure 5 - Post Accreditation Activities 22

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

I. INTRODUCTION

This document is a review of the various programs and processes that should be in place within any organization for the protection of their information assets. The many areas of any organization's security program play key roles in supporting the certification and accreditation (C&A) process of an organization's information assets. The supporting areas along with the C&A and post C&A activities make up an organization's information security program. Five primary sections herein outline an information security program baseline. The first section is a high-level overview of an information security program. The second section identifies the laws and regulations that require an information security program. The third section identifies supporting security standards and best practices. The fourth section gives an overview of the accreditation's supporting programs. The last section address the C&A methodology, an outline of the methodologies output and the post accreditation activities.

II. AUDIENCE

This document is targeted towards the federal (civilian) agency arena; however, health care organizations, corporate organizations, and even branches of the Department of Defense may find it useful. The idea is to provide a reference with an information security program and C&A process baseline. Any of these groups may be able to use the information as a training tool to assist in understanding the components of an information security program and the C&A process. However, the focus is primarily on the federal (civilian) agencies for the establishment of an information security program and C&A process. Corporate organizations and health care organizations may be able to use the information to establish their own programs. However health care organizations must ensure they review the requirements applicable to them as outlined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 (final rule)[1]. The Department of Defense has had a certification program established for a number of years, and even though the information provided here does not apply to their national security systems, it may still be useful in training or at a high level, for program comparison purposes.

[1] United States. Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160 and 164, Standards for Privacy of Individual Identifiable Health Information, December 28, 2000. Pg. 82487

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

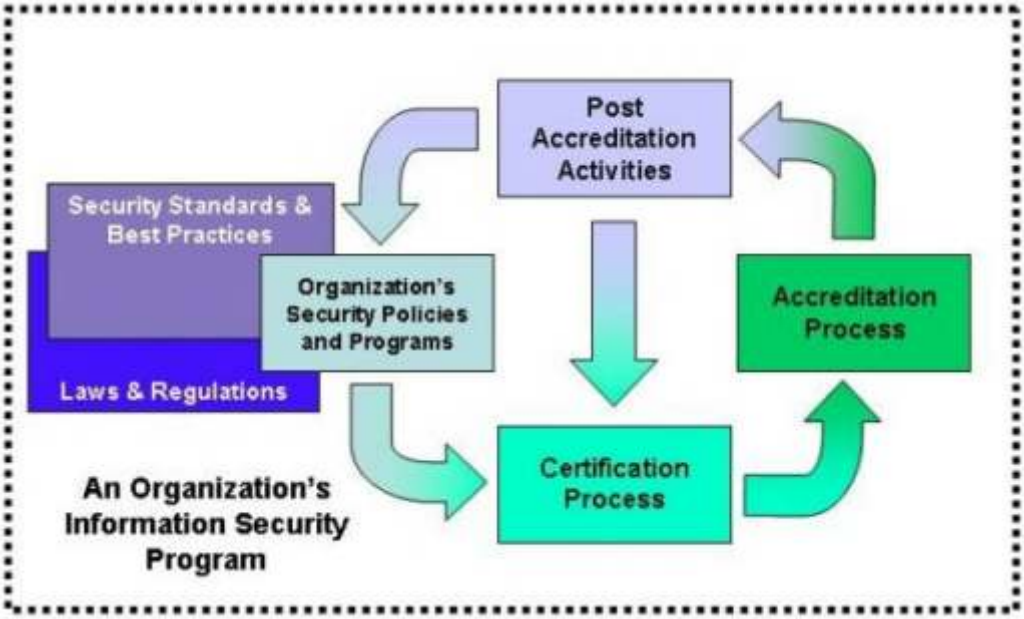

Figure 1 – Overview of an Information Security Program

III. THE INFORMATION SECURITY PROGRAM

An organization builds its security program from the applicable laws, regulations, and standards by developing various organizational policies and programs that create the overall program. Many elements of the Information Security Program are required and validated the authorization of the organization's information systems (Figure 1 - Overview of an Information Security Program). The organization's policies and activities that make up a security program are the responsibility of senior management within an organization, not the sole responsibility of one individual. The Information System Security Officer (ISSO) has overall responsibility of an organization's Information Security Program. Yet other policies and programs developed by other individuals within the organization also support the Information Security Program and the accreditation process.

IV. SECURITY LAWS & REGULATIONS

A. Federal Information Security Management Act

The Federal Information Security Management Act (FISMA) of 2002, which was passed as TITLE X of The Homeland Security Act (signed into law on November 27, 2002) replaced GISRA and repealed The Computer Security Act Section 11332 of Title 40, United States Code. FISMA provides a framework to ensure the security controls used to protect the federal assets are effective and grants more responsibility to the National Institute of Standards and Technology (NIST)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

to develop and maintain standards for minimum information security controls. Compliance with the standards is mandatory[2].

B. Health Insurance Portability and Accountability Act of 1996

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, August 21, 1996. The final rule for HIPAA became effective February 26, 2001. HIPAA outlines that health care systems must establish national standards for the protection of an individual's health information that is privacy related data. The standards should also improve the efficiency and effectiveness of the health care systems electronic exchange of information between organizations/systems. Additionally, the standards will ease the growing concerns of the public regarding the protection of personal medical information.

C. Office of Management and Budget Circular A-130

Office of Management and Budget (OMB) Circular A-130, Appendix III calls for a management authorization for major applications and general support systems to process information[3]. That authorization is based on an assessment of the management, operational, and technical controls put in place to protect an organizations information technology resources. The resources assessed include the hardware, software, data, and people that are part of the business processes supporting the organization's mission(s). The authorization by the management official should occur at least every three years or whenever a major modification of the application or system happens.

Other laws and regulations that may be applicable to an organization and may provide requirements for their information security program are identified below. While this list is not all-inclusive, it does provide a good reference library to establish a requirements matrix.

U.S. Privacy Act, 1974 (as Amended)
U.S. Electronic Communications Privacy Act, October 1986
U.S. Computer Abuse Amendments Act, January 1995
U.S. Economic and Protection of Proprietary Information Act, October 1996
U.S. Kennedy-Kassenbaum Health Insurance and Portability Accountability Act (HIPAA), October 2002
U.S. National Information Infrastructure Protection Act, October 1996
Telecommunications Act of 1996 (Clinger-Cohen Act of 1996)

Additional reference resources that may be helpful can be found at the Chief Information Officers Counsel, IT Related Laws and Regulations web page (quick link - http://www.cio.gov/it related laws and regulations).

---

[2] United States. One Hundred Seventh Congress of the United States, E-Government Act of 2002, January 23, 2003. H.R. 2458-50

[3] United States, Office of Management and Budget (OMB) Circular A-130 Appendix III, Security of Federal Automated Information Resources, December 10, 2002. Section A.3.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

V. SECURITY STANDARDS & BEST PRACTICES

A. National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) has developed a library of guidance and standards (http://csrc.nist.gov/publications/) which can be used to help organize an information security program to protect an organization's information technology assets. The NIST Special Publications (SP), 800 series, established in 1990, provides research and guidance in computer security working with industry, government, and academic organizations. These documents provide approved guidance that the organizations within the federal government are now required to follow[4]. NIST SP 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Systems*, provides a methodology for certifying the security of the technology, policies, and procedures that an organization has in place that protects the confidentiality, integrity, and availability of their information assets[5]. As defined in 44 United States Code (USC), Section 3542, the confidentiality, integrity, and availability of an information asset is:

- Confidentiality – "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"
- Integrity - "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…"
- Availability - "Ensuring timely and reliable access to and use of information…"

Other NIST Publications, which provides guidance for developing different areas of an organization's information security program and support the certification of information systems, are identified below.

- NIST 800-12, *An Introduction to Computer Security*; The NIST Handbook
- NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
- NIST SP 800-53, DRAFT, *Guide to Information Technology Security Services*

---

[4] United States. One Hundred Seventh Congress of the United States, E-Government Act of 2002, January 23, 2003. H.R. 2458-58

[5] Ron R., et al. "NIST SP 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Systems," 2nd Public Draft, June 2003. Pg. 3

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- NIST FIPS PUB 199, DRAFT, *Standards for Security Categorization of Federal Information and Information Systems*
- NIST FIPS PUB 102, *Guideline for Computer Security Certification and Accreditation*

B. International Organization for Standardization

The ISO 17799 standard is a detailed security standard that lists ISO identified best practices of the information security arena. The international standard is composed of two parts, ISO 17799 - a method of practice and BS-7799-2 - specifications for an information management system. The standard is organized into ten major sections covering different aspects of information security.

- Business Continuity Planning
- System Access Control
- System Development and Maintenance
- Physical and Environmental Security
- Compliance
- Personnel Security
- Security Organization
- Computer & Network Management
- Asset Classification and Control
- Security Policy

Many organizations accept the ISO 17799 as reputable standards to use for constructing an information security program.

C. SANS (SysAdmin, Audit, Network, Security)

SANS is an established institute recognized for its research, education, and certification of individuals in the information security profession. SANS also provides a medium for these professionals to share their lessons learned. This community is made of individuals working in government, educational and civil organizations from around the world. SANS supports many ongoing programs to promote secure computing environments using best practices that have been identified, discussed, and validated by the information security professionals. Security Consensus Operational Readiness Evaluation (SCORE) is an effort between SANS and the Center for Internet Security (CIS) to promote these best practices (http://www.sans.org/score/) and make them available to the security community at large.

D. Center for Internet Security

The Center for Internet Security (CIS) is a non-profit organization that provides other organizations methods and tools to improve, measure, monitor, and compare the security status of an organization's Internet-connected systems and

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

appliances[6]. The CIS works with a large member group consisting of vendors and individual users that identify security threats that are of concern to the members in the group. Working with the member community, and as stated by the CIS web page, the CIS makes available *Internet security benchmarks* that are "based on recognized best practices for deployment, configuration, and operation of network systems."[7] The CIS' benchmarks are developed in an attempt to cover three factors in Internet-based attacks: technology, processes, and human behavior. All benchmarks are made available to the public and be found at http://www.cisecurity.org/benchmarks.html.

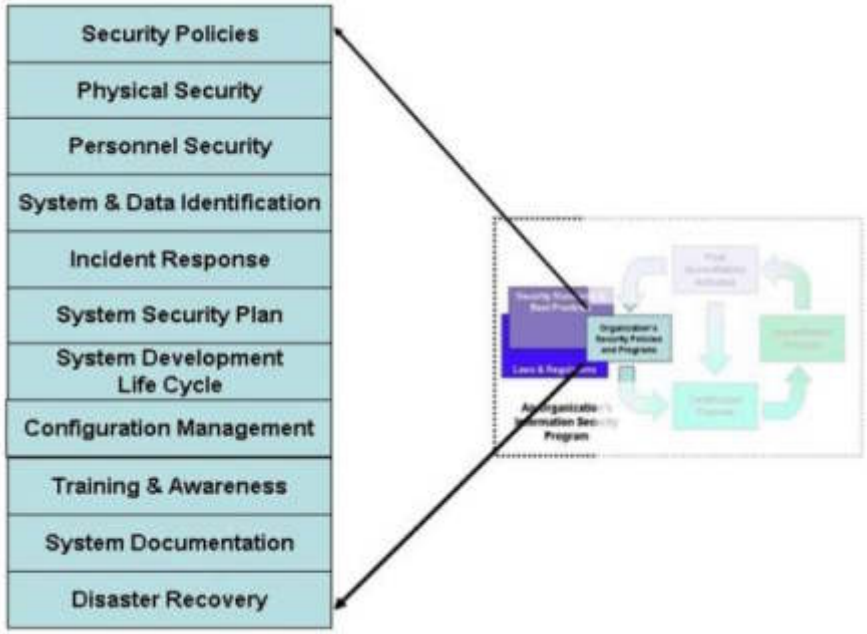

Figure 2 - Organization's Supporting Security Policies & Programs

VI. ORGANIZATION'S SUPPORTING PROGRAMS

An organization will normally have a multitude of different policies and programs, Figure 2 – Organization's Supporting Security Policies & Programs, that may not all be the responsibility of the ISSO. Even so, a large portion of these policies and programs directly or in-directly support an organizations information security program and the certification and accreditation (C&A) of the organization's information systems. The subjects identified here all play some role in the overall protection of organizations information assets and while this list is not all-inclusive, it does help establish an overall security program.

[6] Center for Internet Security Charter, Version 1.23, April 1, 2002, Center for Internet Security. October 20, 2003
[7] Center for Internet Security Charter, Version 1.23, April 1, 2002, Center for Internet Security. October 20, 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

A. Security Policies

A comprehensive information security program requires an approach that reaches beyond the areas that most normal information technology people consider. Senior management has overall responsibility for the protection of an organization's information assets. A comprehensive program begins with a senior management official promulgating an organizational information security policy that establishes, at a high-level, the purpose and scope of the program and defines different organization roles and responsibilities by position. The information security program depends upon the responsibilities and actions of the other offices in performing their responsibilities outlined in the policy which help in the protecting the organizations information assets.

Once the information security policy has been established, specific additional policies will establish support for different specific areas that play a role in protecting the organizations information assets. During the C&A process the policies are used as a reference point to validate that the application or general purpose system meets the requirements outlined within these policies.

Some topic specific policies that should be considered for development that will play a role in protecting an organization's information assets include:

- Security Organization
- System and Data Identification (Assets Classification and Control)
- Personnel Security
- Physical Security
- System Access Control
- Computer and Network Management
- Incident Response
- System Development Life Cycle
- System Configuration Management (hardware and software maintenance)
- Business Continuity Planning and Disaster Recovery Planning.

B. Physical Security

While information security professionals may take actions to secure the logical portions of an organization's information assets, if a system's components are not physically protected from threats, the security professional's actions are all done in vain. Physical threats can be any event that causes a disruption of services provided by an information system for an organization. Threats may be man-made or natural, accidental or intentional. An organization's physical security may include security guards, dogs, and cameras to help monitor and control access to the organization's grounds, building, and designated spaces (i.e. the computer room or data center). Fire and smoke detection and prevention with environmental controls are essential elements that support parts of an organizations physical security. However, even with all these controls in place manual intervention is still required at some point in the physical security

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

realm. Therefore, each of the controls used at an organization should have operating procedures that have been planned, tested, and implemented. Once tested and implemented the operating procedures will guide personnel through required actions during a physical threat.

C. Personnel Security

Another aspect of a security program may require controls in place to reduce risks posed by individuals handling the organization's information that may be sensitive in nature. This sensitivity could be due to information that is proprietary to the organization's products or processes or there may be personal data requiring protection in accordance with the Privacy Act of 1974[8]. In any case, the organization must know that the individuals are qualified and trustworthy. In order to do meet these and other requirements each sensitive position should be clearly defined. This definition should outline the work to be completed, the position's responsibilities, and the sensitivity of the position. To determine a person's trustworthiness for these positions a screening process, sometimes referred to as a background check will be required. A background check may be as simple as calling the local law authorities to check for a police record. On the other hand, the checks may be so extensive it requires investigations into the person's history for the past 10 or more years. The background check would be based on the sensitivity of the position and how much funding the organization wants to pay for the process. Once a person(s) is hired to hold the job position(s), the organization should ensure that these individuals are trained to stay proficient in their responsibilities.

D. System and Data Identification

OMB Circular A-130, Appendix III defines two primary system categories to assist federal agencies in identifying the systems that support their mission[9].

> **"general support system** or **system** - an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO)."
>
> **"major application** - means 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. Note: All Federal applications require some level of

[8] United States. Privacy Act of 1975, 5 USC Sec. 552a (as amended), September 26, 2003.
[9] United States, Office of Management and Budget (OMB) Circular A-130 Appendix III, Security of Federal Automated Information Resources, December 10, 2002. Section A.2.c and Section A.2.d.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate."

Based on the definitions a general support system is easy to identify however, the major application description has ambiguity that may require an organization to further clarify an identification process to indicate which of their systems are major applications. The identification of they system helps determine the impact of a loss or compromise[10] if it were to occur. Therefore, each organization should have a formal documented process in place that helps identify which of their systems are major applications. Factors for consideration in the process may include one or more of the following items.

- The importance of the system or information to the organization's business process or mission.
- Financial harm to the organization if the system or information where compromised.
- Cost of a systems development, maintenance, and replacement.
- Cost of the information's development, maintenance, and replacement.
- Harm to the organization's reputation if the system or information where compromised.
- Would there be a loss of life or limb if the system or information where compromised.

The organization's business managers and system users will conduct each system's identification process since these individuals have a better understanding of how the loss or compromise of the asset's confidentiality, integrity, or availability would affect the organization. NIST has recently promulgated a draft document that provides standard security categories to help identify impact to an organization when there is a loss or compromise of an organization's information assets. Although this publication is in draft form as of October 2003, it is projected for publication prior to 2004.

E. Incident Response Program

An incident response program is essential for any organization that has any automated system supporting any facet of their business process[11]. The program should be chartered through the organizations information security policies and clearly define the goals of the program granting the authority needed to make the decisions and take the actions required when in the best interest of the organization. The policy should be coordinated with the organization's senior

[10] National Institute of Standards and Technology, Federal Information Processing Standards (FIPS) Publication (PUB) 199, Standards for Security Categorization of Federal Information and Information Systems, Pre-Publication Final, December 2003. Pg. 1

[11] United States. One Hundred Seventh Congress of the United States, E-Government Act of 2002, January 23, 2003. H.R. 2458-53

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

management to ensure the incident response team has approval from the different internal organizations that may be affected by an incident.

A well-formulated incident response program will be multifaceted with a specific team of individuals who have the training, the talents, and the equipment to respond to a computer related anomaly in a timely and effective manner. While technical ability is the fore thought for a computer response team, the organizations legal staff and public affairs office should be included within the team in case there are legal implications or public involvement. Prior to any incident, documentation supporting the program should be in place outlining actions for the different phases. As identified in SANS "Computer Security Incident Handling Step By Step" guide[12] there are six phases that an incident response program should have outlined are:

- Preparation
- Identification
- Containment
- Eradication
- Recovery, and
- Follow-up

Any incident is an undesired event for an organization and having a well thought out incident response program provides a layer of protection for an organization providing logical steps to keep the event from escalating out of control.

F. System Security Plan

The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls that are in place or those controls that are planned for meeting the security requirements. The system security plan also delineates responsibilities and expected behavior of all the individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for the system. It should reflect input from the various managers who are responsible for the system. This includes the information owners, the system operators, the system security manager, and the system administrators. Once developed the system security plan plays a key role in providing an overview of the system for the C&A process.

At a minimum, the system security plan should cover the subjects outlined below to keep within the NIST standards[13].

- SYSTEM IDENTIFICATION
    - System Name/Title

[12] The SANS Institute, Computer Security Incident Handling Step By Step, *Version 1.5,* May 1998.
[13] Swanson, M. "NIST SP 800-18, Guide for Developing Security Plans for Information Systems," December 1, 1998.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Responsible Organization
- Information Contact(s)
- Assignment of Security Responsibility
- System Operational Status
- General Description/Purpose
- System Environment
- System Interconnection/Information Sharing
- Applicable Laws or Regulations Affecting the System
- General Description of Information Sensitivity

- MANAGEMENT CONTROLS
  - Risk Assessment and Management
  - Review of Security Controls
  - Rules of Behavior
  - Planning for Security in the Life Cycle
  - Authorize Processing

- OPERATIONAL CONTROLS
  - Personnel Security
  - Physical and Environmental Protection
  - Production, Input/Output Controls
  - Contingency Planning
  - Application Software Maintenance Controls
  - Data Integrity/Validation Controls
  - Documentation
  - Security Awareness and Training
  - Incident response capability

- TECHNICAL CONTROLS
  - Identification and Authentication
  - Logical Access Controls
  - Public Access Controls
  - Audit Trails

The system owner is responsible for maintaining the security plan. Any time there are changes to the system, the security plan should be reviewed and updated as applicable. At a minimum, this should be done on an annual basis. The organizations information security personnel should ensure that the system owners stick to the review and update process since this document should be the first item they review when a system is being assessed in the C&A process.

G. System Development Life Cycle

The System Development Life Cycle (SDLC) is a traditional process using a set of logical systematic activities, also known as phases, to develop, implement, and operate a system. Each of the phases have specific activities that integrates the implementation of security into the life cycle process of a system that will

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

make the security controls more effective and potentially reduce the cost of security for the system. NIST identifies five common phases[14] in the SDLC process that have some security related actions.

- Initiation Phase
- Acquisition/Development Phase
- Implementation Phase
- Operation/Maintenance Phase
- Disposition Phase

H. Configuration Management

Configuration management involves the identification of a system's configuration at given points in time, systematically controlling changes to the configuration, and maintaining the integrity and traceability of the system configuration throughout the systems lifecycle. The items that should be placed under a configuration management program include the software and hardware products that comprise the system as well as items required to create or maintain these products. A configuration management program should address the following items:

- Identify the proper process for making system changes
- Identify the individuals and organization that made changes to the system
- Identify the changes that were made to the system
- Document when the changes were made to the system
- Document the justification of the changes made to the system
- Document who requested and authorized the system changes

The CM process includes procedures, hardware associated with or supporting the system, software applications, and all network physical and logical configurations and documentation affecting the system. The processes will serve to reduce the discrepancy between what is authorized and what is implemented. The CM process will ensure that the operational system is implementing the correct security policy as promulgated by the organizations security requirements.

I. Training and Awareness Program

OMB[15] and FISMA[16] require that each federal organization establish a training program where all personnel within an organization are thoroughly trained in their security responsibilities. An information security-training program accomplishes

[14] Grance, T. et al. NIST SP 800-64, Security Considerations in the Information System Development Life Cycle, October 2003. Pg. 6

[15] United States, Office of Management and Budget (OMB) Circular A-130 Appendix III, Security of Federal Automated Information Resources, December 10, 2002. Section A.3.a.(2)(b) and A.3.b.(2)(b)

[16] United States. One Hundred Seventh Congress of the United States, E-Government Act of 2002, January 23, 2003. H.R. 2458-26

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

this for the organization. This program should be established through the organization's information security policy. This lets all personnel know that the organization's senior management feels security is important and that everyone will be held accountable for their actions. The training program is the process through which the organization informs the users of the organization's security policies and practices, what is expected of the users, and how the users are to handle the organization's information, data, and systems. The training program should provide the relevant and needed security skills and competency to enable the organization's employees, contractors, and partners to perform their jobs more effectively. Learning methods or activities should concentrate on a particular topic; those topics should be rotated to prevent a particular topic from becoming stale and unnoticed. Topics are not limited and change as technology advances. Some of the NIST[17] recommended topics include, but are not limited to the following items:

- Password usage and management – including creation, frequency of changes, and protection
- Protection from viruses, worms, Trojan horses, and other malicious code – scanning, updating definitions
- Policy – implications of noncompliance
- Unknown e-mail/attachments
- Web usage – allowed versus prohibited; monitoring of user activity
- Spam
- Data backup and storage – centralized or decentralized approach
- Social engineering
- Incident response – contact whom? "What do I do?"
- Shoulder surfing
- Changes in system environment – increases in risks to systems and data (e.g., water, fire, dust or dirt, physical access)
- Inventory and property transfer – identify responsible organization and user responsibilities (e.g., media sanitization)
- Personal use and gain issues – systems at work and home
- Handheld device security issues – address both physical and wireless security issues
- Use of encryption and the transmission of sensitive/confidential information over the Internet – address agency policy, procedures, and technical contact for assistance
- Laptop security while on travel – address both physical and information security issues
- Personally owned systems and software at work – state whether allowed or not (e.g., copyrights)
- Timely application of system patches – part of configuration management

[17] Wilson, M. et al. NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, October 2003. Pg 24-25

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Software license restriction issues – address when copies are allowed and not allowed
- Supported/allowed software on organization systems – part of configuration management
- Access control issues – address least privilege and separation of duties
- Individual accountability – explain what this means in the organization
- Use of acknowledgement statements – passwords, access to systems and data, personal use and gain

An organization's information security training is one of the most important aspects of computer and information security, building on awareness. An effective training and awareness program reduces the number of accidental security incidents because people are more conscious of general security issues.

J. System Documentation

As a part of any organizations well defined SDLC process, the development of documentation specific to the system should be outlined. The documentation would outline the system from development to it's' production state. The documentation may include items identified below.

- system functional requirements,
- database software configurations,
- data dictionary,
- operating system configurations,
- user application configuration,
- system architecture (physical),
- data flow (logical),
- system interconnections,
- user manuals,
- system security plan,
- a disaster recovery/business continuity plan,
- security test plan,
- certification statement, and
- any service level agreements, memorandums of understanding, or memorandums of agreement that was required for the system.

The documentation will support the organizations information security program through its availability allowing authorized and qualified individuals the ability to understand the system configurations and operational state. This assists problem isolation reducing system downtime and provides a baseline for the development of enhancements for the system in the future. Having the right documentation available keeps an organization from depending on the individual(s) who developed the system. The system owner is the party

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

responsible to ensure that the documentation is developed, maintained, and made available to the appropriate people.

K. Disaster Recovery

Disaster recovery consists of two areas, a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP). The two areas are established to ensure that an organization's critical business processes are maintained to support the organization's primary mission. The BCP provides a strategy to minimize the after effects of a disruptive event while the DRP consist of the actions that must be taken before, during and after a disruption for each system supporting a business process to minimize the losses to the organization. While the goals and actions in these plans are extremely important, the people carrying out these activities are the most critical elements. The plans must ensure that the organization's personnel are the most important asset and that loss of life or limb outweighs any loss of information or physical asset owned by the organization. Once these plans have been completed, it is extremely important that these plans be proven through testing. Therefore, every plan needs to be tested! The results of the testing will provide lessons learned that would be used to strengthen the plans correcting weaknesses or oversights.

VII. CERTIFICATION AND ACCREDITATION (C&A) PROGRAM

The C&A of an information system is the process where an independent party verifies that a system meets or exceeds the security requirements identified for protecting an organization's information system and data. The method used for verification is usually similar no matter who completes the process and consist of five basic steps: identify assets, identify threats and vulnerabilities, collect data (test, inspect, and interview), analyze the data and document the results. Once the results are documented a senior management official reviews and approves, or disapproves the operation of the system based on the results of the verification process.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

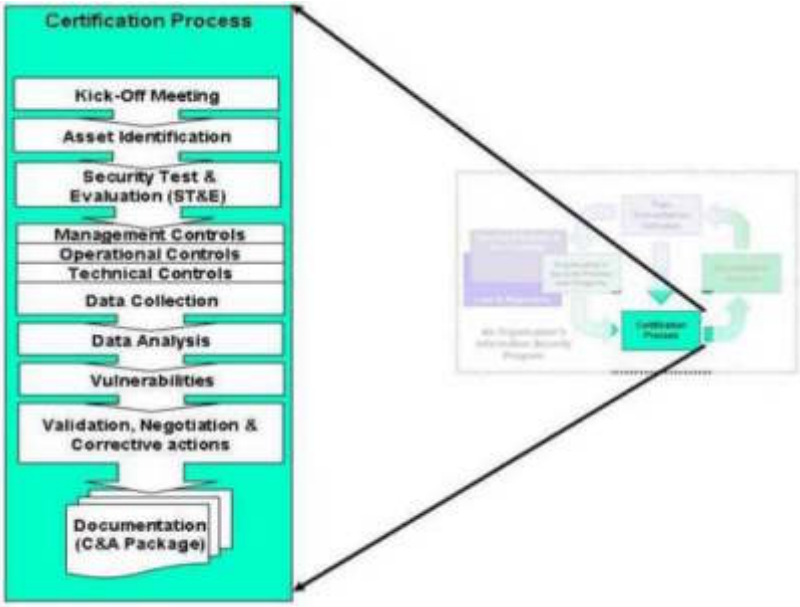

Figure 3 - An Information System's Certification Process

A. Certification Process

The certification process, Figure 3 – An Information System's Certification Process, consist of activities using established techniques that verify that the system's security controls as documented in the system's security plan have been implemented and are effective in mitigating risks to the system. The process takes into consideration a system's operating environment and should identify the other compensating controls in place to protect the system. Another outcome of this process is the identification of vulnerabilities within the system and recommendations to correct the vulnerability.

One of the first things to accomplish should be a "kick-off" meeting. This meeting is to get the system support personnel and the security personnel, or certification team, together for an introductory of all personnel involved. The primary objective of this meeting is for the certification team to review the process with the system owner, system security officer, system technical point of contact, and system administrator(s). The meeting provides a forum for all personnel to meet each other discuss the process and make known the rules of engagement for the activities and the materials (documentation) needed for the review and validation processes.

Asset & Threat Identification. The system's security plan should be reviewed for a description of the system, its security controls, its physical and logical interconnectivity, and the operational environment the system operates within. Threats to the system may also be listed in the system's security plan however, if they are not, they should be identified at this point in the process. A walk through should be conducted to visually identify the system's physical components being certified and how the components are interconnected. At this point, the scope of

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

the system's certification begins to formulate. The scope is to include clear identification of boundaries for testing and any test information that can be reused for other systems at the organization. The certification team may want to meet with the system owner and other applicable personnel to inform them of assets that have been identified, and the scope of the certification process.

Familiarization with the assets and their environment will help the certification team determine how the system will be certified and what testing will be conducted for the certification process. A system certification may reuse data from another certification or supply data for other system certifications. This data reuse is accomplished in one of two different situations. One situation would be when you are deploying a specific type of system where the security controls are specific to that system and are not changed no matter where the system is installed. This data is system specific and referred to as type-specific data. The other situation is where you have multiple systems at one location, or site, and you have security controls specific to that site and are applicable for all systems at that one location. This data would be site-specific data. The Department of Defense has used this process during the certification of many of their information systems which saving time and expenses. NIST has also identified this as a viable means to reuse evaluation data that may be applicable to several systems[18].

A security test and evaluation (ST&E) plan sometimes referred to as a test plan, can then be defined for the certification team's activities. A very simplistic test plan may look something like Table VII-1, Sample Test Plan, shown on the next page. The test plan can be used as a guide for validating the implementation of the systems security controls that are in place. The control areas to be tested are those security controls described in the system's security plan: the Management, Operational, and Technical Controls. Each control area has several sub-areas that are more specific and should be tested during the certification process. The plan could identify the method used to test each specific control area being reviewed. Test methods include visual inspections, personnel interviews, documentation review, and use of automated tools that are applicable. The test could also include the potential tool(s) required to conduct the testing and the personnel involved.

[18] Ron R., et al. "NIST SP 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Systems," 2nd Public Draft, June 2003, Pg. 14

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

	Control	Test Method	Tool	Personnel
Management Controls	Risk Assessment & Management	Interview Inspection	Checklist	System Owner Computer Security Team
	Review of Security Controls	Interview Doc Review	Checklist	System Owner Computer Security Team
	Rules of Behavior	Inspection	Checklist	System Owner
	Planning for SDLC	Interview Doc Review	Checklist	System Owner System Developer
	Authorize Processing	Interview Doc Review	Checklist	System Owner Computer Security Team
Operational Controls	Personnel Security	Interview Inspection	Checklist	System Owner Administrative Officer
	Physical & Environmental Protection	Interview Inspection Doc Review	Checklist	Facilities Administrator System Owner
	Production, Input/Output	Interview Inspection	Checklist	System Owner System Developer
	Contingency Planning, Disaster Recovery	Interview Inspection Doc Review	Checklist	Facilities Administrator System Owner System Administrator Computer Security Team
	Application Software Maintenance	Interview Inspection Doc Review	Checklist	System Owner System Administrator System Developer
	Data Integrity/Validation	Interview Inspection	Checklist	System Owner System Administrator System Developer
	Documentation	Interview Doc Review	Checklist	System Owner System Developer Computer Security Team Administrative Officer
	Security Awareness & Training	Interview Doc Review	Checklist	System Owner Information System Security Officer
	Incident Response Capability	Interview Doc Review	Checklist	Information System Security Officer
Technical Controls	Identification & Authentication	Test Inspection	Host and Network Scanning Tools	System Administrator Network Administrator
	Logical Access Controls	Test Inspection	Host and Network Scanning Tools	System Administrator Network Administrator
	Public Access Controls	Test Inspection	Host and Network Scanning Tools	System Administrator Network Administrator
	Audit Trails	Test Inspection	Host and Network Scanning Tools	System Administrator Network Administrator

Table VII-1, Sample Test Plan

Data Analysis. Once the data has been collected it must then be organized and analyzed based on the requirements and considering the known existing threats to the system. The analysis should help determine:

- That the security control meets requirements
- If the security control is implemented as documented
- If the security control is appropriate to protect the system and data
- Any known vulnerabilities

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- What, if any, corrective actions can be taken to correct or reduce the risk which a vulnerability allows
- What other controls are in place to help mitigate risks to the system

Once the analysis is completed and the potential risk levels have been identified for each vulnerability the certification team should meet with the system owner and the applicable personnel to validate the findings and eliminate any false positives or negatives. During this process negotiations regarding the vulnerabilities risk levels may occur, along with the system owner taking actions to correct vulnerabilities. Either way, these actions may change the vulnerabilities that were originally identified during the certification process therefore changing the overall risk level of the system. All vulnerabilities, corrected and outstanding should be documented to maintain a system history of the systems configuration changes through out its life cycle. This documentation also feeds the certification report used in the accreditation of the system.

Certification & Accreditation Package – The output of the certification process is the C&A package document. The C&A package documents the results from the security testing and evaluation and provides the authorizing official with the information needed to make a decision based on the risk level of the system as to whether the system should be authorized for operation. The package must include the results of the testing, an accreditation letter, the system's security plan, and a plan of actions and milestones for corrective actions (Fix-It Plan). A package, which includes the items listed below, should provide all the appropriate information for the DAA to make an accreditation decision.

Executive Summary – This document is from the certifying authority and addressed to the designated approving authority (DAA) summarizing the results of the certification process, outlining the level of risk of the system, identifying any outstanding actions that are required and provides the certifier's certification recommendation.

DAA Brief – This document is the formal presentation used to present the executive summary and describes, at a high level the results of the system certification process.

Accreditation Letter – This document is the official letter to the system owner from the DAA and is the DAA's formal accreditation statement that informs the system owner of their responsibilities in maintaining the accreditation of the system.

Risk Acceptance Letter – This document is an agreement between the system owner and the certifier. The letter documents the level of risk that has been identified for the system. The letter will outline the system owner's responsibility to ensure that the system's security posture is maintained in its current environment. It also tells the system owner that any changes to the system

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

should be reviewed by the computer security office for potential vulnerabilities that may change the system's level of risk.

Risk Assessment Report – This document should describe the system's risk level based on the security controls that are in place to mitigate any vulnerability that have been identified and associated to threats for the system.

Security Test & Evaluation Results – The ST&E results are the documented out put from the various steps completed in the ST&E work plan.

Risk Definitions – This document identifies the systems threats and associated risks. Risk calculation methodology can also be defined herein.

Fix-It Plan – This document summarizes all the identified vulnerabilities and can be potentially used as a work plan for corrective actions. This document, if formatted appropriately, can be used to track the status of any vulnerability and whether it has been accepted and will be mitigated, transferred or ignored.

System Diagram – This document identifies the systems architecture at the time it was subjected to the certification process. The diagram can identify any logical and physical connections and indicate the boundaries that were determined for the scope of the certification activities.

Acronyms – This document can be included as an appendix to the main report and list any applicable acronyms that are used through out.

References – This document can be included as an appendix to the main report and list any references that are applicable to the report or the processes involved.

System Security Plan – This document should be a copy of the system's security plan that describes the system and the security controls that are in place to protect the system.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

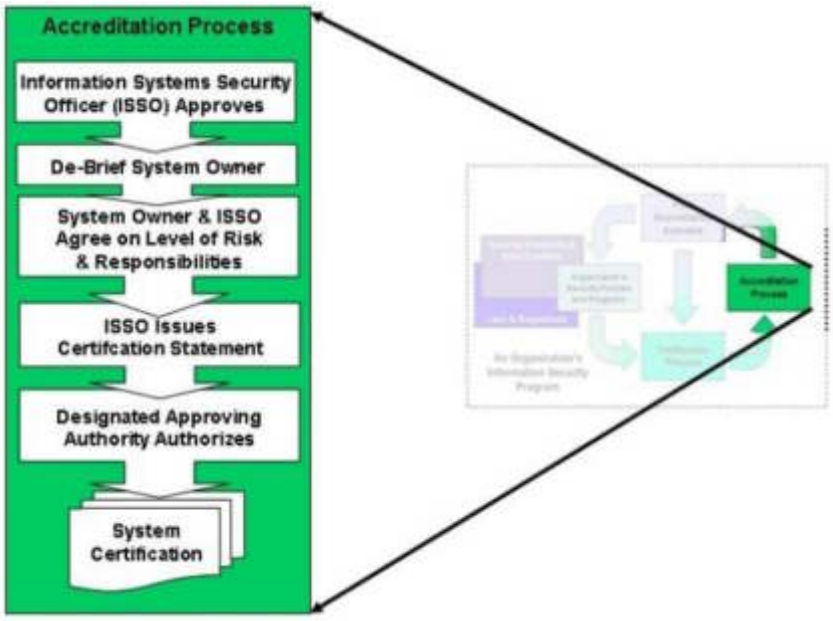

Figure 4 - An Information System's Accreditation Process

B. Accreditation Process

The certification process provides the documentation of identified vulnerabilities that the certification team and the system owner have reviewed, corrected, and negotiated. Results are documented in the C&A package and undergo an accreditation process such as that indicated in Figure 4, An Information System's Accreditation Process. The C&A package should be provided to the ISSO for review allowing feedback and approval of the certification teams output from the certification process. The system owner would then be briefed on the C&A package as completed, to include any recommendations or changes that may have been made during the ISSO's review. Prior to the certifying officer issuing a certification statement, the system owner and certifying officer should be in agreement on the system's overall level of risk, pending corrective actions and each parities responsibility in completing these actions. The agreement of the system's risk level and plan to reduce or eliminate any remaining risk to the system by all responsible parties should help the decision process confronting the designated approving authority.

With the C&A package previously outlined, there should be enough information for the DAA to make a decision for the operation of the system. The DAA's decision is risk-based, and done with the knowledge that the system may have remaining vulnerabilities that pose residual risk to the organization's remaining assets and operations. After the DAA reviews the C&A package, the system can be accepted or rejected due to the residual risk that the system poses. If rejected, the DAA's concerns should be corrected if possible. The system will then be re-evaluated to verify that controls have been put in place to eliminate or reduce the risk that was previously identified. If accepted an accreditation statement is issued for the system. There are two types of accreditations that

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

may be issued for a system: 1) approval to operate (ATO) or 2) intermediate approval to operate (IATO). The ATO indicates that the system has been approved for period of time, typically a period of three years[19] or when significant changes are made to the system's architecture. The IATO indicates that a system has a limited approval for a specific period of time that is determined by the approving authority and may be based on the risk level of the system. For a system with an IATO, the goal is controls are put in place for vulnerabilities identified so that at the end of the specified period the system can be accredited with an ATO.

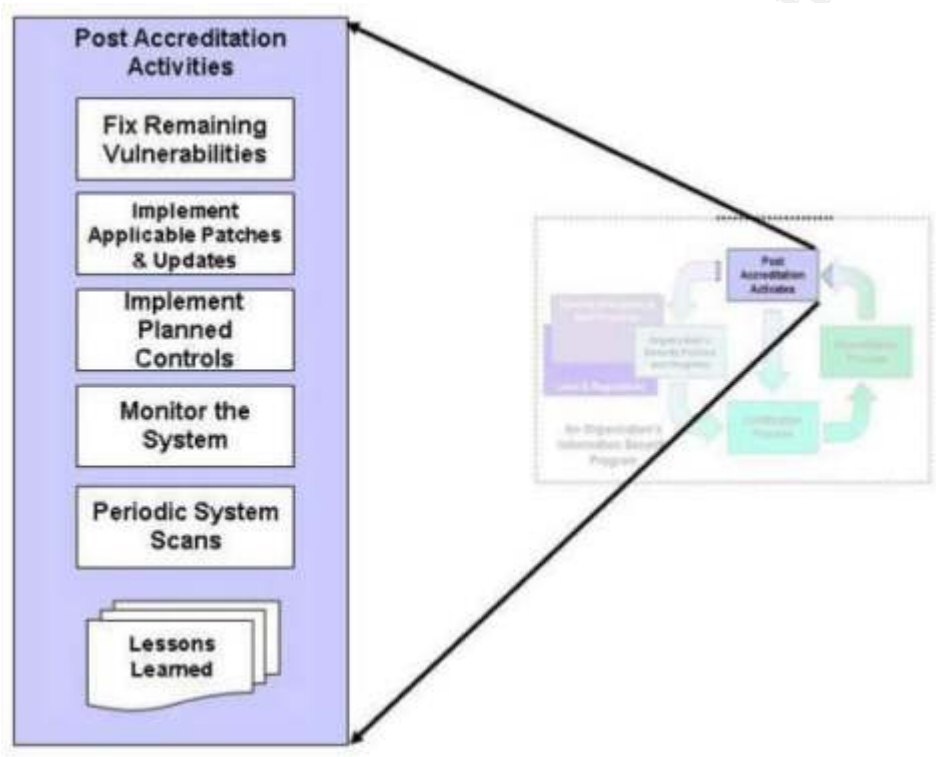

Figure 5 - Post Accreditation Activities

C. Post Accreditation Activities

Several post activities should be accomplished after the accreditation of an information system, Figure 5 – Post Accreditation Activities. During the C&A process documentation should have a proposed "Fix- it Plan" developed as a part of the C&A package. After the system has been accredited, the fix-it plan can be used as a management tool for tracking corrective actions that need to be completed to correct the vulnerabilities identified during the system's C&A process. The system should also be subject to applicable patches and updates that become available for the operating system, middleware and any other applications or components of the system. The patches and updates should be

[19] United States, Office of Management and Budget (OMB) Circular A-130 Appendix III, Security of Federal Automated Information Resources, December 10, 2002, Section A.3.a.(3) and Section A.3.b.(4)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

tested in a development environment prior to implementing in the production environment. This testing will help determine what changes could be made to the system when the patch or update is installed to make sure no other vulnerabilities are introduced to the system. This testing scenario should also include planned changes or controls that had not yet been implemented. The accredited systems should also be scheduled for scans conducted no less than annually to ensure that the integrity of the system's technical security posture has not changed from what was identified during the certification process. Additionally, the organization should consider implementing an active monitoring program to alert appropriate personnel (i.e. technical or security staff) of any unauthorized or undesired activities that may be occurring to the organization's systems. All of these post accreditation activities help identify and mitigate risks to an organizations information systems. All activities can provide lessons learned which could be used to support new organizational policies, policy changes, and program development and implementation. The same lessons learned can also provide input into the certification process for future systems or re-accreditation processes.

VIII. SUMMARY

Some of the areas supporting the information security program may be required by law or regulations where others may be considered a best practice. To help meet these requirements the information security policy could be promulgated from an organization's senior executive. This informs management that the organization takes information security seriously. The policy could identify the other department's responsibilities, through their policies or programs, in the protection of the organizations information assets. The verification that these policies and programs are being implemented effectively an organization means having the information systems subjected to the C&A review process. The C&A process can provide the organization feedback on how well they are meeting or exceeding regulatory or organizational requirements. NIST has published a small library providing guidance that an organization can use in the development of their information security program. While these documents are not required by the commercial sector, they can still be used to establish a sound program.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

Center for Internet Security Charter, Version 1.23, April 1, 2002, Center for Internet Security. October 20, 2003 http://www.cisecurity.org/charter.html

Grance, T. et al. NIST SP 800-64, Security Considerations in the Information System Development Life Cycle, October 2003 http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf

National Institute of Standards and Technology, Federal Information Processing Standards (FIPS) Publication (PUB) 199, Standards for Security Categorization of Federal Information and Information Systems, Pre-Publication Final, December 2003 http://csrc.nist.gov/publications/drafts/draft-fips-pub-199.pdf

Ron R., et al. "NIST SP 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Systems," 2nd Public Draft, June 2003 http://csrc.nist.gov/publications/drafts/sp800-37-Draftver2.pdf

Swanson, M. "NIST SP 800-18, Guide for Developing Security Plans for Information Systems," December 1, 1998 http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF

The SANS Institute, *Computer Security Incident Handling Step By Step, Version 1.5,* May 1998 https://store.sans.org//store_item.php?item=62

United States. Privacy Act of 1975, 5 USC Sec. 552a (as amended), September 26, 2003 http://www.usdoj.gov/foia/privstat.htm

United States. Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160 and 164, Standards for Privacy of Individual Identifiable Health Information, December 28, 2000 http://www.cms.hhs.gov/hipaa/hipaa2/regulations/privacy/finalrule/PvcFR01.pdf

United States. One Hundred Seventh Congress of the United States, E-Government Act of 2002, January 23, 2003 http://www.cio.gov/documents/e_gov_act_2002.pdf

United States. Office of Management and Budget (OMB) Circular A-130 Appendix III, Security of Federal Automated Information Resources, December 10, 2002 http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

Wilson, M. et al. NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, October 2003 http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**