CHAPTER

11

Security Component Fundamentals for Assessment

The key to the management, oversight, and governance of the security components and program in the organization is the understanding of the risks involved and how each is treated and tolerated by the organization. As the assessor for a US governmental system, it is important to grasp and work with the fundamental requirements for these systems. With the SP 800-53 structured approach to security controls, the assessor can review each management, technical, and operational area of security directly. NIST SP 800-53, rev. 4, is divided into 18 control families comprising 3 security classes of controls:

1. *Management controls*: Focus on the management of the computer security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management, through policy and documentation.
2. *Operational controls*: Address security issues related to mechanisms primarily implemented and executed by people (as opposed to systems). Often, they require technical or specialized expertise and rely on management activities as well as technical controls.
3. *Technical controls*: Technical controls are security controls that are configured within the system. They can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

Each family of controls starts with the base "–1" control which defines the policies necessary for the family of controls. All 18 families of controls within the SP 800-53 are defined in this manner. These are commonly known as the "XX-1 Policy and Procedures" controls. An information security policy is an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information. Information security policy is an essential component of information security governance – without the policy, governance has no substance and rules to enforce.

Information security policy should be based on a combination of appropriate legislation, such as FISMA; applicable standards, such as NIST Federal Information Processing Standards (FIPS) and guidance; and internal agency requirements. Therefore, the assessor will identify the relevant governmental documents for each policy and then check the system

documentation for reference to those documents. Agency information security policy should address the fundamentals of agency information security governance structure, including:

1. Information security roles and responsibilities
2. Statement of security control baseline and rules for exceeding the baseline
3. Rules of behavior that agency users are expected to follow and minimum repercussions for noncompliance

We will discuss each of these families of controls in this chapter, starting with the management controls.

MANAGEMENT AREAS OF CONSIDERATION

There are many areas which the assessor needs to consider when evaluating and testing the various management controls installed on the systems under test as shown below in the listing of the families of controls. The starting point for most of these areas is the oversight and governance requirements. So the first area of management controls to review would be the security program and its operations section.

The management areas covered by SP 800-53 controls are varied and wide in their scope.

The basic ideas behind the controls are to provide direct information security program elements to assist managers in establishing, implementing, and running an information security program. Typically, the organization looks to the program for overall responsibility to ensure the selection and implementation of appropriate security controls and to demonstrate the effectiveness of satisfying their stated security requirements.

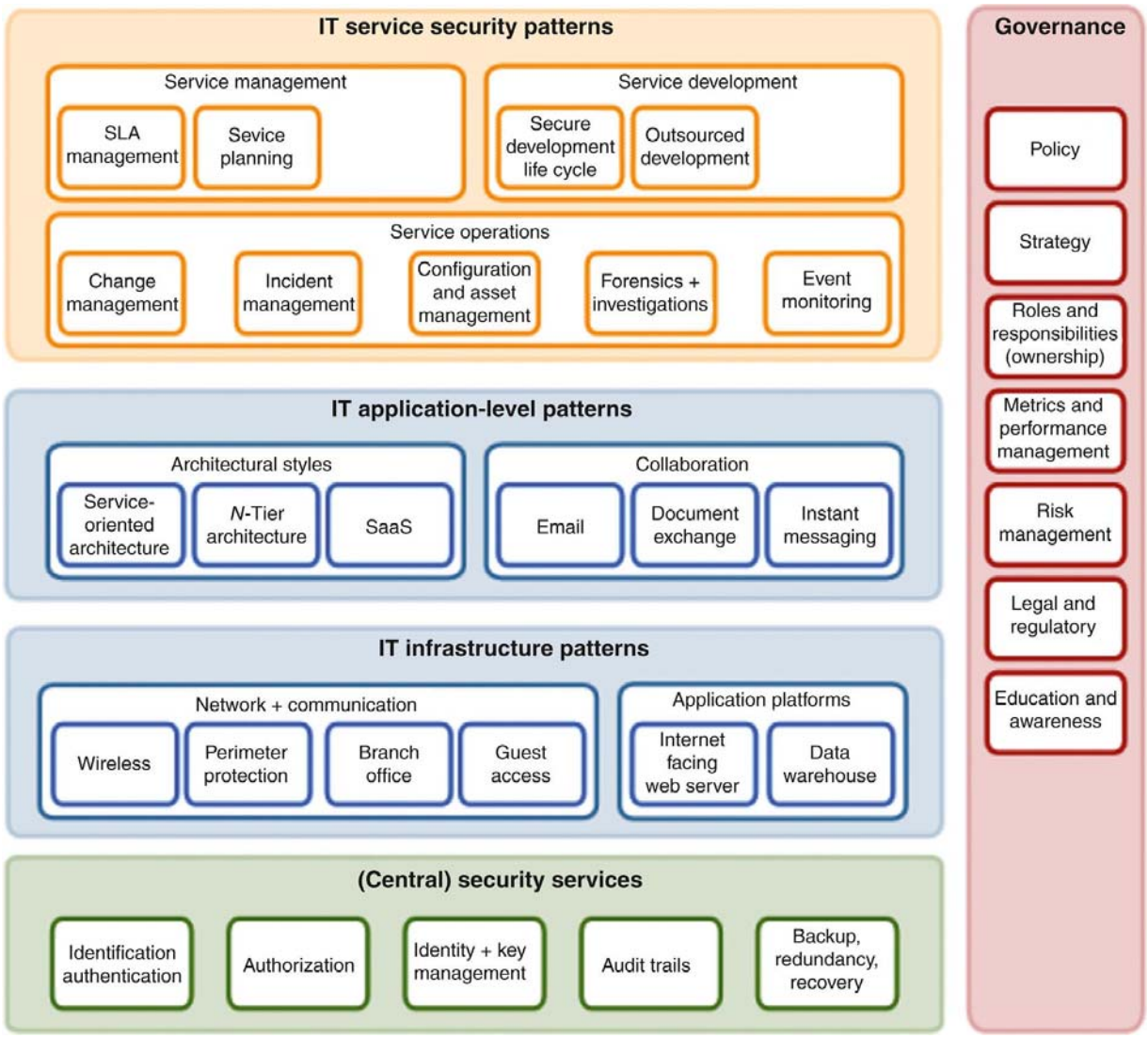
As SP 800-100 states: "Federal agencies rely heavily on information technology (IT) to run their daily operations and deliver products and services. With an increasing reliability on IT, a growing complexity of federal government IT infrastructure, and a constantly changing information security threat and risk environment, information security has become a mission-essential function. This function must be managed and governed to reduce the risks to federal government operations and to ensure the federal government's ability to do business and serve the American public."[1]

Key elements to review for any security management program are as follows:

- *Senior management commitment and support*: As the cornerstone for successful establishment and continuance of an information security management program, commitment and support from senior management should exist.
- *Policies and procedures*: As a structured framework, policy and procedures start with a general organization policy providing concise top management declaration of direction.
- *Organization*: Responsibilities for the protection of individual assets and for carrying out specific security processes should be clearly defined. The information security policy should provide general guidance on the allocation of security roles and responsibilities in the organization.

[1]SP 800-100, p. 2.

- *Security awareness and education*: All employees of an organization and, where relevant, third-party users should receive appropriate training and regular updates on the importance of security in organizational policies and procedures.
- *Monitoring and compliance*: In assessing the effectiveness of an organization's security program(s) on a continuous basis, IS auditors must have an understanding of the organization's monitoring activities in assessing the effectiveness of security programs and controls established.
- *Incident handling and response*: A computer security incident is an adverse event that threatens some aspect of computer security.



While the standards such as NIST, ISO, and Information Security Forum (ISF) divide their materials into chapters, these do not translate into a security architecture landscape very well.

Therefore, the Open Security Architecture Forum[2] proposes an architecture that identifies topics of poor coverage, determines priorities for new patterns, and helps the community coordinate their risk management (RM) activities. Open Security Architecture (OSA) is a not-for-profit organization, supported by volunteers for the benefit of the security community.

MANAGEMENT CONTROLS

The management controls are defined in SP 800-53 as the overarching controls needed for oversight, compliance, and acquisition of security components, equipment, and processes for security within a federal system. The basic structure of controls is to define the security action to be taken, supplemental guidance for use and installation of the control, any enhancements to each control, references, and then the parameters or variables that the organization can use to install and implement the control.

Program Management (PM)

Information Security Program Plan

The information security program plan can be represented in a single document or compilation of documents at the discretion of the organization. The plan documents the organization-wide PM controls and organization-defined common controls. The security plans for individual information systems and the organization-wide information security program plan together provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system (IDS) providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.

Critical Infrastructure Plan

The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources (CIKR) protection plan. Critical infrastructure assets are essential for the functioning of a society and economy. Most commonly associated with the term are facilities for:

1. Electricity generation, transmission, and distribution
2. Gas production, transport, and distribution
3. Oil and oil products production, transport, and distribution
4. Telecommunication
5. Water supply (drinking water, waste water/sewage, stemming of surface water (e.g., dikes and sluices))
6. Agriculture, food production and distribution

[2]Retrieved from http://www.opensecurityarchitecture.org on 1/21/2015.

7. Heating (e.g., natural gas, fuel oil, district heating)
8. Public health (hospitals, ambulances)
9. Transportation systems (fuel supply, railway network, airports, harbors, inland shipping)
10. Financial services (banking, clearing)
11. Security services (police, military)

The main document of the US government for the critical infrastructure is HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, which references the CIKR of the United States.

Essential Services that Underpin American Society

It is the policy of the United States to enhance the protection of our nation's CIKR against terrorist acts that could:

1. Cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction
2. Impair federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety
3. Undermine state and local government capacities to maintain order and to deliver minimum essential public services
4. Damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services
5. Have a negative effect on the economy through the cascading disruption of other CIKR
6. Undermine the public's morale and confidence in our national economic and political institutions

Industrial Control Systems Characteristics

- Pervasive throughout critical infrastructure
- Need for real-time response
- Extremely high availability, predictability, and reliability

An industrial control system (ICS) is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. ICSs include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and programmable logic controllers (PLC). ICS are typically found in the electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries as well as in air and rail transportation control systems.

Security PM is designed to and often struggles with meeting several and often conflicting requirements:

- Minimizing risk to the safety of the public
- Preventing serious damage to environment
- Preventing serious production stoppages or slowdowns

- Protecting critical infrastructure from cyber attacks and human error
- Safeguarding against compromise of proprietary information

So the assessor must review the program documents, reports, and reviews to verify the documented requirements are actually being met while the A&A – controls review and implementation process reflects the security is being maintained during operational activities.

INFORMATION SECURITY RESOURCES

The assessor will determine if the organization:

1. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement
2. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required
3. Ensures that information security resources are available for expenditure as planned

Organizations may designate and empower an Investment Review Board (IRB; or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process. Which ties into the Capital Planning and Investment Control (SP 800-65) criteria of an Exhibit 300 must be submitted for all major investments in accordance with this section.

Major information technology (IT) investments also must be reported on the agency's Exhibit 53. Exhibit 300s and the Exhibit 53, together with the agency's Enterprise Architecture (EA) program, define how to manage the IT Capital Planning and Control Process.

All IT investments must clearly demonstrate the investment is needed to help meet the agency's strategic goals and mission. They should also support the President's Management Agenda (PMA). The capital asset plans and business cases (Exhibit 300) and "Agency IT Investment Portfolio" (Exhibit 53) demonstrate the agency management of IT investments and how these governance processes are used when planning and implementing IT investments within the agency.

Investments in the development of new or the continued operation of existing information systems, both general support systems and major applications, proposed for funding in the President's budget must:

1. Be tied to the agency's information architecture. Proposals should demonstrate that the security controls for components, applications, and systems are consistent with and an integral part of the IT architecture of the agency.
2. Be well planned, by:
   a. Demonstrating that the costs of security controls are understood and are explicitly incorporated in the life-cycle planning of the overall system in a manner consistent with OMB guidance for capital programming
   b. Incorporating a security plan that discusses risk management.
3. Manage risks, by:
   a. Demonstrating specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time

   b. Demonstrating specific methods used to ensure that the security controls are commensurate with the risk and magnitude of harm that may result from the loss, misuse, or unauthorized access to or modification of the system itself or the information it manages
   c. Identifying additional security controls that are necessary to minimize risks to and potential loss from those systems that promote or permit public access, other externally accessible systems, and those systems that are interconnected with systems over which program officials have little or no control
4. Protect privacy and confidentiality, by:
   a. Deploying effective security controls and authentication tools consistent with the protection of privacy, such as public key–based digital signatures, for those systems that promote or permit public access
   b. Ensuring that the handling of personal information is consistent with relevant government-wide and agency policies, such as privacy statements on the agency's websites
5. Account for departures from NIST guidance. For non-national security applications, to ensure the use of risk-based cost-effective security controls, describe each occasion when employing standards and guidance that are more stringent than those promulgated by the NIST.

To promote greater attention to security as a fundamental management priority, OMB continues to take steps to integrate security into the capital planning and budget process. To further assist in this integration, the Plan of Action and Milestones (POAMs; M02-01) and annual security reports and executive summaries must be cross-referenced to the budget materials sent to OMB in the fall including Exhibits 300 and 53.

MEASURES OF PERFORMANCE (SP 800-55)

NIST SP 800-55 is a guide to assist in the development, selection, and implementation of measures to be used at the information system and program levels. These measures indicate the effectiveness of security controls applied to information systems and supporting information security programs. Such measures are used to facilitate decision making, improve performance, and increase accountability through the collection, analysis, and reporting of relevant performance-related data – providing a way to tie the implementation, efficiency, and effectiveness of information system and program security controls to an agency's success in achieving its mission. The performance measures development process described in SP 800-55 will assist agency information security practitioners in establishing a relationship between information system and program security activities under their purview and the agency mission, helping to demonstrate the value of information security to their organization.

Additionally, performance measurements are required to ensure the IT system is in compliance with existing laws, rules, and regulations, such as FISMA.

Factors that must be considered during the development and implementation of an IT measurement program are as follows:

- Measures must yield quantifiable information: percentages, averages, and numbers.
- Data that supports the measures needs to be readily obtainable.

- Only repeatable information security processes should be considered for measurement.
- Measures must be useful for tracking performance and directing resources.

MEASURES OF PERFORMANCE

- Metric types
- Metrics development and implementation approach
- Metrics development process

Metric Types

- "Am I implementing the tasks for which I am responsible?"
- "How efficiently or effectively am I accomplishing those tasks?"
- "What impact are those tasks having on the mission?"

Metrics Development Process

The place of information security metrics within a larger organizational context demonstrates that information security metrics can be used to progressively measure implementation, efficiency, effectiveness, and the business impact of information security activities within organizations or for specific systems.

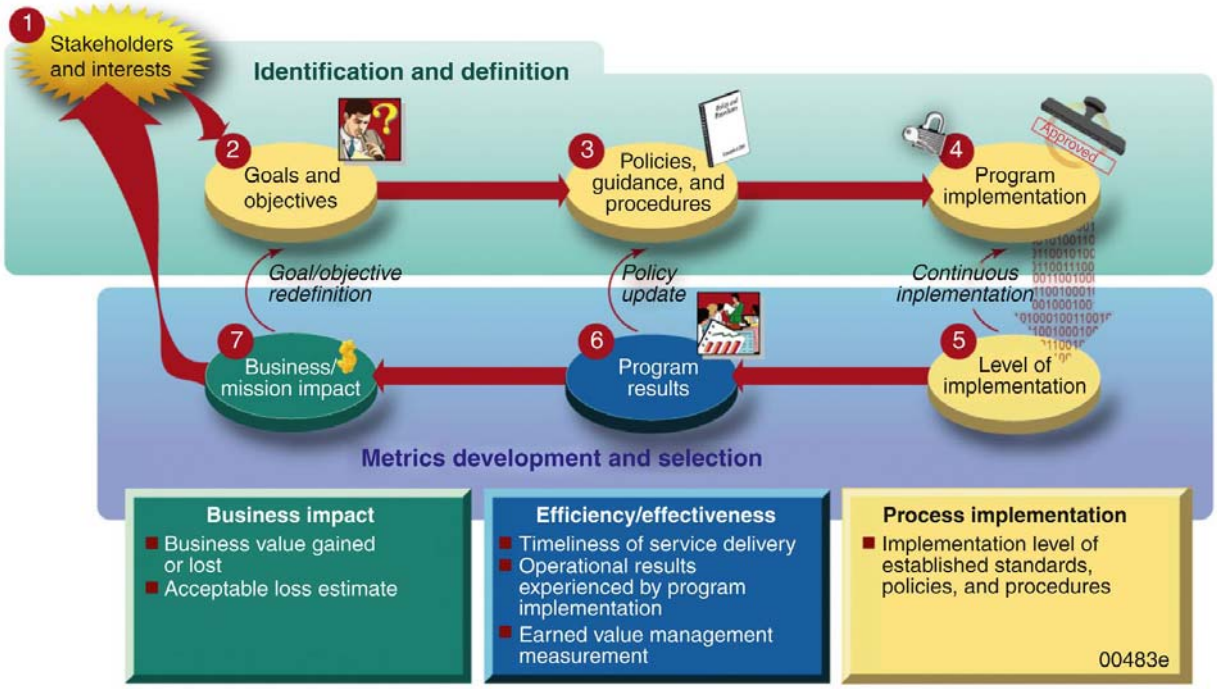
The information security metrics development process consists of two major activities:

1. Identifying and defining the current information security program
2. Developing and selecting specific metrics to measure implementation, efficiency, effectiveness, and the impact of the security controls

The process steps do not need to be sequential. Rather, the process illustrated in the following diagram provides a framework for thinking about metrics and aids in identifying metrics to be developed for each system. The type of metric depends on where the system is within its life cycle and on the maturity of the information system security program. This framework facilitates tailoring metrics to a specific organization and to the different stakeholder groups present within each organization.

Phases 5, 6, and 7 involve developing metrics that measure process implementation, effectiveness and efficiency, and mission impact, respectively. The specific aspect of information security that metrics will focus on at any given point will depend on information security program maturity. Implementation evidence, required to prove higher levels of effectiveness, will change from establishing existence of policy and procedures to quantifying implementation of these policies and procedures, then to quantifying results of implementation of policies and procedures, and ultimately to identifying the impact of implementation on the organization's mission.

Based on existing policies and procedures, the universe of possible metrics can be prohibitively large; therefore, agencies should prioritize metrics to ensure that the final set selected for initial implementation has the following attributes:

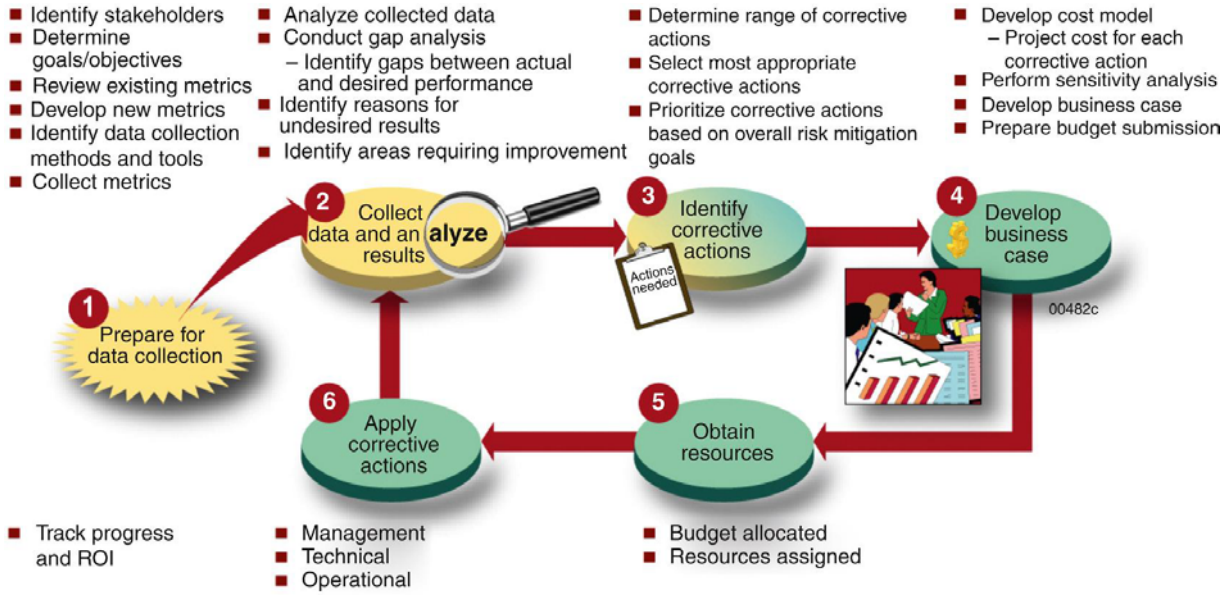


1. Facilitates improvement of high-priority security control implementation. High priority may be defined by the latest Government Accountability Office (GAO) or Inspector General (IG) reports, results of a risk assessment, or an internal organizational goal.
2. Uses data that can realistically be obtained from existing processes and data repositories.
3. Measures processes that already exist and are relatively stable. Measuring nonexistent or unstable processes will not provide meaningful information about security performance and will therefore not be useful for targeting specific aspects of performance. On the other hand, attempting such measurement may not be entirely useless, because such a metric will certainly produce poor results and will therefore identify an area that needs improvement.

Metrics can be derived from existing data sources, including security certification and accreditation, security assessments, POAM, incident statistics, and agency-initiated or independent reviews. Agencies may decide to use a weighting scale to differentiate the importance of selected metrics and to ensure that the results accurately reflect existing security program priorities. This process would involve assigning values to each metric based on the importance of a metric in the context of the overall security program. Metrics weighting should be based on the overall risk mitigation goals, is likely to reflect higher criticality of department-level initiatives versus smaller-scale initiatives, and is a useful tool that facilitates integration of information security into the departmental capital planning process.

A phased approach may be required to identify short-, mid-, and long-term metrics in which the implementation time frame depends on a combination of system-level effectiveness, metric priority, data availability, and process stability. Once applicable metrics that contain the qualities described above are identified, they will need to be documented with

supporting detail, including frequency of data collection, data source, formula for calculation, implementation evidence for measured activity, and a guide for metric data interpretation. Other information about each metric can be defined based on an organization's processing and business requirements.



Metrics Program Implementation

- Prepare for data collection.
- Collect data and analyze results.
- Identify corrective actions.
- Develop business case and obtain resources.
- Apply corrective actions.

FEDERAL ENTERPRISE ARCHITECTURE

As part of the management criteria for controls and the system under review, the federal requirement defined in the Clinger Cohen Act of 1996 requires all systems be included in the EA for the agency. This process is identified and delineated in the Federal Enterprise Architecture (FEA) process as adopted by the federal CIO Council.

The FEA practice adopted three core principles to guide its strategic direction. They are as follows:

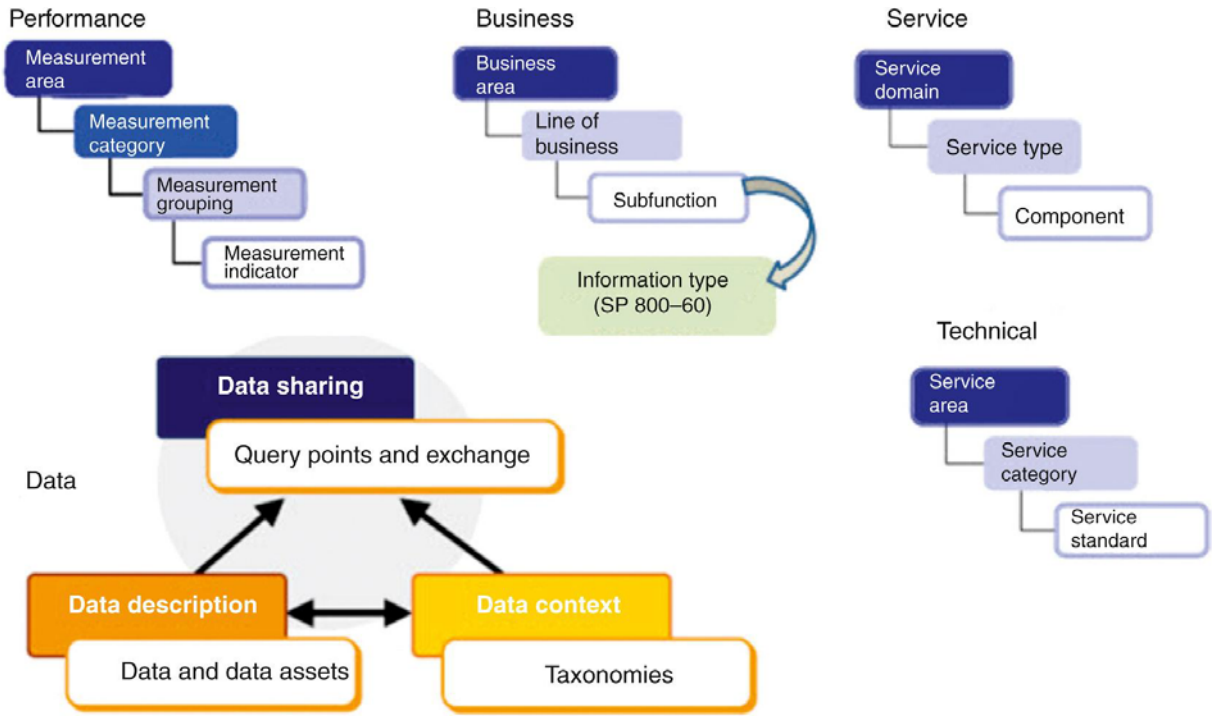
1. *Business-driven*: The FEA is most useful when it is closely aligned with government strategic plans and executive-level direction. Agency mission statements, presidential management directives, and agency business owners give direction to each agency's EA and to the FEA.

2. *Proactive and collaborative across the federal government*: Adoption of the FEA is achieved through active participation by the EA community in its development and use. The FEA community is responsible for the development, evolution, and adoption of the FEA.
3. *Architecture improves the effectiveness and efficiency of government information resources*: Architecture development is an integral part of the capital investment process. No IT investment should be made without a business-approved architecture.

The FEA consists of a set of interrelated "reference models" designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across agencies. Collectively, the reference models comprise a framework for describing important elements of the FEA in a common and consistent way.

Through the use of this common framework and vocabulary, IT portfolios can be better managed and leveraged across the federal government. This chapter introduces the purposes and structures of the five FEA reference models:

1. Performance Reference Model (PRM)
2. Business Reference Model (BRM)
3. Service Component Reference Model (SRM)
4. Technical Reference Model (TRM)
5. Data Reference Model (DRM)



Information protection needs are technology-independent, required capabilities to counter threats to the organization through the compromise of information (i.e., loss of confidentiality, integrity, or availability).

Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational RM strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs.

The security categorization process is used to make such potential impact determinations, which is related to and feeds the development of the security categorization requirements for each system as found in FIPS-199, guided by SP 800-60. These reference the process defined in the first step of the Risk Management Framework (RMF) as for in the previous chapters.

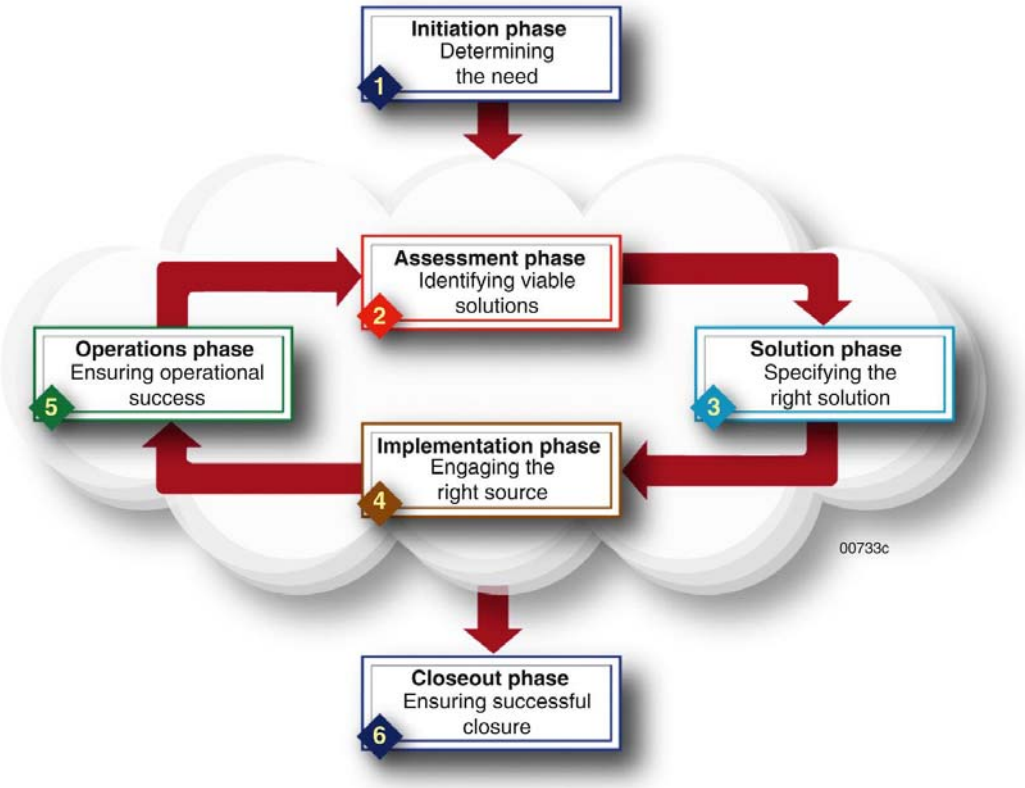
SYSTEM AND SERVICES ACQUISITION (SA)

From OMB Budget Circular A-11, the Exhibit 300 is the capture mechanism for all of the analyses and activities required for full internal review (e.g., IRB, CIO). More importantly, Exhibit 300 is the document that OMB uses to assess investments and ultimately make funding decisions, and therefore should be leveraged by agencies to clearly demonstrate the need for life cycle and annual funding requests. Following selection into the agency's IT portfolio, the agency aggregates Exhibit 300s into the Exhibit 53. The Exhibit 53 provides an overview of the agency's entire IT portfolio by listing every IT investment, life cycle, and budget-year cost information.

Exhibit 300s are companions to an agency's Exhibit 53. Exhibit 300s and the Exhibit 53, together with the agency's EA program, define how to manage the IT Capital Planning and Control Process. Exhibit 53A is a tool for reporting the funding of the portfolio of all IT investments within a department while Exhibit 300A is a tool for detailed justifications of major "IT investments." Exhibit 300B is for the management of the execution of those investments through their project life cycle and into their useful life in production.

By integrating the disciplines of architecture, investment management, and project implementation, these programs provide the foundation for sound IT management practices, end-to-end governance of IT capital assets, and the alignment of IT investments with an agency's strategic goals. As architecture-driven IT investments are funded in the "invest" (development/acquisition) phase, they move forward into the implementation phase where system development life-cycle processes are followed and actual versus planned outputs, schedule, and operational performance expenditures are tracked utilizing performance-based management processes.

SECURITY SERVICES LIFE CYCLE



SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, provides a foundation on which organizations can establish and review IT security programs. The eight Generally Accepted System Security Principles in SP 800-14 are designed to provide the public or private sector audience with an organization-level perspective when creating new systems, practices, or policies.

General Considerations for Security Services

- *Strategic/mission*
- *Budgetary/funding*
- *Technical/architectural*
- *Organizational*
- *Personnel*
- *Policy/process*

To facilitate identification and review of these considerations, security program managers may use a set of questions when considering security products for their programs.

1. Identify the user community.
2. Define the relationship between the security product and the organization's mission.
3. Identify data sensitivity.
4. Identify an organization's security requirements.
5. Review security plan.
6. Review policies and procedures.
7. Identify operational issues such as daily operation, maintenance, and training.

This then leads to the assessor reviewing the acquisition criteria for various security components, services, and equipment along with the documentation, contract requirements, and the varied support design reports and analyses to ensure there are considerations defined for selecting the information security products and services from the following viewpoints:

- Organizational
- Product
- Vendor
- Security checklists for IT products
- Organizational conflict of interest

INFORMATION SECURITY AND EXTERNAL PARTIES

The security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties should be maintained, and should not be reduced by the introduction of external-party products or services. Any access to the organization's information processing facilities and processing and communication of information by external parties should be controlled. Where there is a business need for working with external parties that may require access to the organization's information and information processing facilities, or in obtaining or providing a product and service from or to an external party, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed to and defined in an agreement with the external party.

These external party arrangements can include:

- Service providers, such as internet service providers (ISPs), network providers, telephone services, and maintenance and support services
- Managed security services
- Customers
- Outsourcing facilities and/or operations, for example, IT systems, data collection services, and call center operations
- Management and business consultants, and auditors
- Developers and suppliers, for example, of software products and IT systems
- Cleaning, catering, and other outsourced support services
- Temporary personnel, student placement, and other casual short-term appointments

CA – SECURITY ASSESSMENT AND AUTHORIZATION

This is the control family for the RMF and its implementation. So an assessor will review and identify all the components of the RMF, the identities of the key roles and the people assigned those roles, the process functions, and the key organizational documents which the agency has produced to support these RMF processes as identified in the previous chapters of this book and in SP 800-37, rev. 1.

PL – PLANNING FAMILY AND FAMILY PLANS

The assessor must ensure the organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals. Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises. Organizational advance planning and coordination includes both emergency and nonemergency (i.e., planned or nonurgent unplanned) situations.

This process is documented in the System Security Plan (SSP) which will include the organizational rules of behavior for each user of the system under review and the system hardware and software inventory.

System Security Plan

The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to organizational operations and assets, individuals, other organizations, and the nation if the plan is implemented as intended.

Rules of Behavior

These establishes and makes readily available to all information system users the rules that describe their responsibilities and expected behavior with regard to information and information system usage, and receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

Information Security Hardware

The organization:

1. Develops an information security architecture for the information system that:
   a. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information

   b. Describes how the information security architecture is integrated into and supports the EA
   c. Describes any information security assumptions about, and dependencies on, external services
2. Reviews and updates the information security architecture periodically to reflect updates in the EA

RA – RISK ASSESSMENT FAMILY

Risk Management

- RM is the process of balancing the risk associated with organizational or business activities with an adequate level of control that will enable the business to meet its mission and/or objectives.
- RM is the identification, assessment, and prioritization of risk followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of adverse events or to maximize the realization of opportunities.

Holistically, RM covers all concepts and processes affiliated with managing risk, including the systematic application of management policies, procedures, and practices; the tasks of communicating, consulting, and establishing the context; and identifying, analyzing, evaluating, treating, monitoring, and reviewing risk.

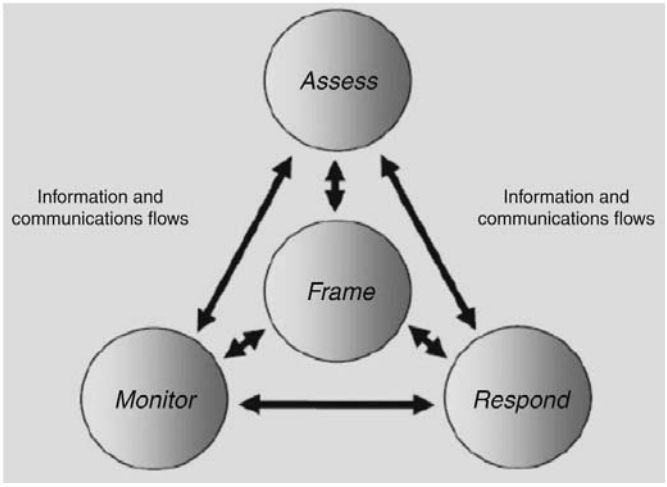
As an assessor, one area to always focus on during the review of the policy and procedural documentation, as well as during the key personnel interviews, is the area of responsibility versus accountability. These are typically defined as follows:

- *Responsibility*: Belongs to those who must ensure that the activities are completed successfully
- *Accountability*: Applies to those who either own the required resources or have the authority to approve the execution and/or accept the outcome of an activity within specific RM processes

The risk factors formula is usually a good place to start the review of risks and how they are viewed and treated within the organization. The formula is relatively straightforward for the organization to use and can be a key element to the organizational risk posture as the assessor reviews and interviews the various management staff during the assessment. The formula is as follows: risk = $T \times V \times \$ \times C$, where C = likelihood × impact. Here:

1. T = threats to the organization
2. V = vulnerabilities within the organization
3. \$ = assets being protected
4. C = consequences of risk

The risk assessment family of controls provides areas of focus for the organization and the assessor to review and update their security posture on an ongoing basis throughout the life cycle of the system under review.



Security Categorization

- A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity, or availability.
- The organization conducts the security categorization process as an organization-wide activity with the involvement of the chief information officer, senior information security officer, information system owner, mission owners, and information owners/stewards. The organization also considers potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts in categorizing the information system. The security categorization process facilitates the creation of an inventory of information assets, and, in conjunction with configuration management (CM)-8, a mapping to the information system components where the information is processed, stored, and transmitted.

Risk and Vulnerability Assessments

- A clearly defined authorization boundary is a prerequisite for an effective risk assessment. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to organization. They also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities).
- In accordance with OMB policy and related e-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems.

- Risk assessments (either formal or informal) can be conducted by organizations at various steps in the RMF including information system categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring.
- RA-3 is a noteworthy security control in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the RMF. Risk assessments can play an important role in the security control selection process during the application of tailoring guidance for security control baselines and when considering supplementing the tailored baselines with additional security controls or control enhancements.

RA-5 Vulnerability Scanning

- The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers).
- Vulnerability scanning includes scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms.
- The organization considers using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.
- The Common Weakness Enumeration (CWE) and the National Vulnerability Database (NVD) are also excellent sources for vulnerability information. In addition, security control assessments such as red team exercises are another source of potential vulnerabilities for which to scan.

The assessor then evaluates the organizational risk tolerance process, usually based on the guidance from SP 800-39 and implemented through the RMF process defined in SP 800-37, rev. 1, for overall treatments of risk within the organization as found through the implementation of the security controls on the system under review. He or she, the assessor, then reviews what is important to the agency and the operations by determining the critical success factors from the management perspective.

CRITICAL SUCCESS FACTORS TO INFORMATION SECURITY MANAGEMENT

- Managers and employees within an organization often tend to consider information security as a secondary priority if compared with their own efficiency or effectiveness matters, because these have a direct and material impact on the outcome of their work.
- For this reason, a strong commitment and support by the senior management on security training is needed, over and above the aforementioned role concerning the information security policy.
- Management must demonstrate a commitment to security by clearly approving and supporting formal security awareness and training (AT). This may require special

management-level training, since security is not necessarily a part of management expertise. The security training for different functions within the organization needs to be customized to address specific security needs. Different functions have different levels of risk. Application developers need technical security training, whereas management requires training that will show the linkage between information security management and the needs of the organization.

- A second vital point is that a professional risk-based approach must be used systematically to identify sensitive and critical information resources and to ensure that there is a clear understanding of threats and risks. Thereafter, appropriate risk assessment activities should be undertaken to mitigate unacceptable risks and ensure that residual risks are at an acceptable level.

OPERATIONAL AREAS OF CONSIDERATION

There are many areas which the assessor needs to consider when evaluating and testing the various operation controls installed on the systems under test as shown below in the listing of the families of controls. The starting point for most of these areas is the user. The user of the system is often, as I teach in my classes, both the first line of defense and the first line of offense with respect to security on the system. So the first area of operational controls to review would be the security awareness, training, and education section.

OPERATIONAL SECURITY CONTROLS KEY CONCEPTS

- AT
- CM
- Contingency planning (CP)
- Incident response (IR)
- Maintenance (MA)
- Media protection (MP)
- Physical and environmental protection (PE)
- Personnel security (PS)
- System and information integrity (SI)

Awareness and Training

With the three areas of awareness, training, and education typically defined in an organizational context by the personnel or human resources department, it is important to focus on the areas of security training being provided to the organization. Concentrate the assessing efforts on the four groups of students for the training. These groups are as follows:

1. End users
2. System administrators – elevated privilege users
3. Security personnel
4. Executives – senior management

Each of these groups has unique security training requirements and we need to ensure these are being addressed by the organization in its training and awareness program. Keep in mind that in several industrial verticals, these training requirements are mandated by either statutory or regulatory requirements, such as the DOD 8570 Workforce regulatory guidance and the end user training requirement found in the Computer Security Act from 1987.

NIST has developed two Special Publications on training of users and support personnel: SP 800-50, *Building an Information Technology Security Awareness and Training Program*, published in October 2003; and SP 800-16, *A Role-Based Model for Federal Information Technology/Cyber Security Training* – third and final draft version from March 2014. Each of these publications provides detailed and explicit information on training and security awareness educational efforts for users, system administrators, security personnel, and executive-level managers.

> A successful IT security program consists of: 1) developing IT security policy that reflects business needs tempered by known risks; 2) informing users of their IT security responsibilities, as documented in agency security policy and procedures; and 3) establishing processes for monitoring and reviewing the program.
>
> Security awareness and training should be focused on the organization's entire user population. Management should set the example for proper IT security behavior within an organization. An awareness program should begin with an effort that can be deployed and implemented in various ways and is aimed at all levels of the organization including senior and executive managers. The effectiveness of this effort will usually determine the effectiveness of the awareness and training program. This is also true for a successful IT security program.
>
> An awareness and training program is crucial in that it is *the* vehicle for disseminating information that users, including managers; need in order to do their jobs. In the case of an IT security program, it is *the* vehicle to be used to communicate security requirements across the enterprise.
>
> An effective IT security awareness and training program explains proper rules of behavior for the use of agency IT systems and information. The program communicates IT security policies and procedures that need to be followed. This must precede and lay the basis for any sanctions imposed due to noncompliance. Users first should be informed of the expectations. Accountability must be derived from a fully informed, well-trained, and aware workforce.[3]

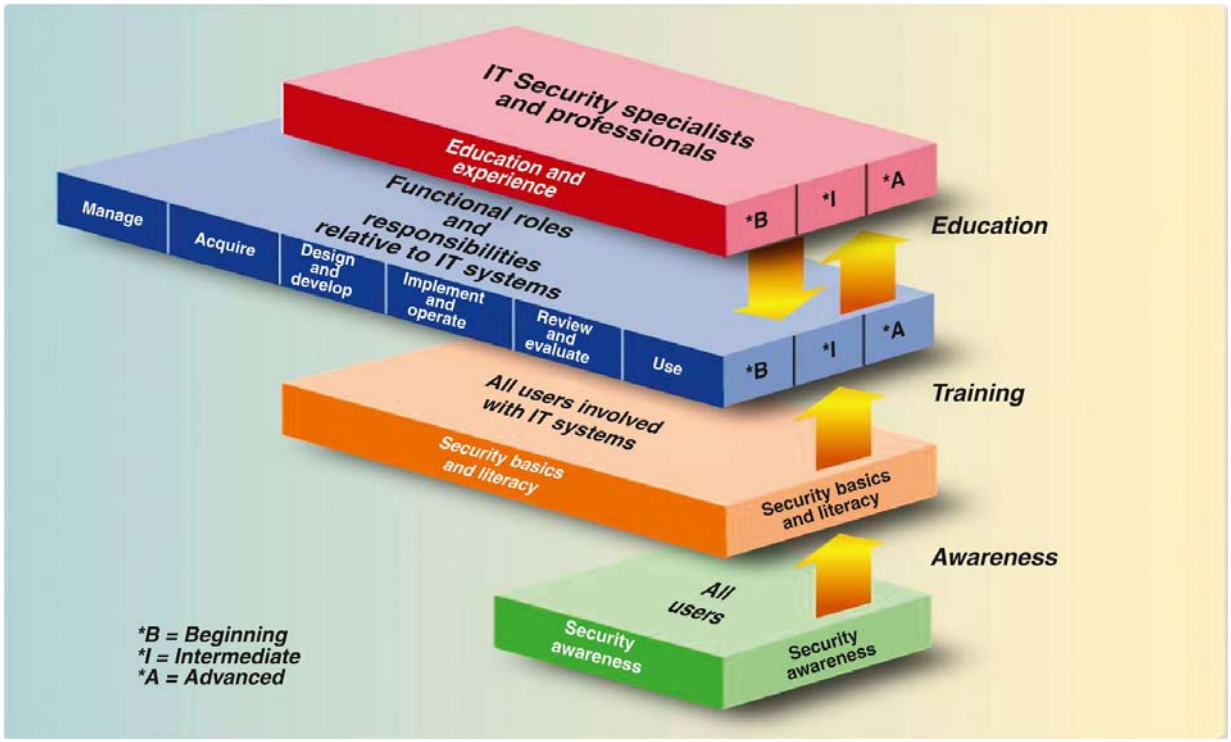
Learning is a continuum; it starts with awareness, builds to training, and evolves into education. The basic construct for this continuum is shown as follows and is found in SP 800-16 and SP 800-50:

Awareness

Security awareness efforts are designed to change behavior or reinforce good security practices. Awareness is defined in NIST Special Publication 800-16 as follows: "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance."

An example of a topic for an awareness session (or awareness material to be distributed) is virus protection. The subject can simply and briefly be addressed by describing what a virus is, what can happen if a virus infects a user's system, what the user should do to protect the system, and what the user should do if a virus is discovered.

[3]SP 800-50, p. 7.



Training

Training is defined in NIST Special Publication 800-16 as follows: "The 'Training' level of the learning continuum strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing)." The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues. The skills acquired during training are built upon the awareness foundation, in particular, upon the security basics and literacy material. A training curriculum must not necessarily lead to a formal degree from an institution of higher learning; however, a training course may contain much of the same material found in a course that a college or university includes in a certificate or degree program.

An example of training is an IT security course for system administrators, which should address in detail the management controls, operational controls, and technical controls that should be implemented. Management controls include policy, IT security PM, RM, and lifecycle security. Operational controls include personnel and user issues, CP, incident handling, AT, computer support and operations, and physical and environmental security issues. Technical controls include identification and authentication (IA), logical Access Controls (ACs), audit trails, and cryptography.

Education

Education is defined in NIST Special Publication 800-16 as follows: "The 'Education' level integrates all of the security skills and competencies of the various functional specialties into

a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response."

An example of education is a degree program at a college or university. Some people take a course or several courses to develop or enhance their skills in a particular discipline. This is training as opposed to education. Many colleges and universities offer certificate programs, wherein a student may take two, six, or eight classes, for example, in a related discipline, and is awarded a certificate on completion. Often, these certificate programs are conducted as a joint effort between schools and software or hardware vendors. These programs are more characteristic of training than education. Those responsible for security training need to assess both types of programs and decide which one better addresses identified needs.[4]

Configuration Management

One of the major areas of focus for any assessor is system changes and CM. There have been many occurrences I have reviewed wherein the development team and the operations team supporting systems have instituted upgrades and changes to system which altered or removed security components with no security review or sign-off on the validity or viability of the change. I have personally seen where the end users requested a change to a processing system to speed up the processing time and the development staff accomplished this through removing the required encryption on the transactional data, and it was approved and installed. The security staff had no idea this change was installed until they scanned the system and found multiple errors in the FIPS-140 and Secure Sockets Layer (SSL) areas where the encryption processing had been removed.

Security CM involves the systems, the hardware and software inventories, the changes to systems, and their interchange with the users on a daily basis. Each change has a security component and all reviews and evaluations of system changes require security checks, configuration reviews, and component evaluations to ensure all the currently installed security controls are maintained and not altered by the proposed change. If a control is modified by the change, detailed engineering and operational examination is needed to make the system safe and secure if the change is approved and installed. All of this activity, usually under the control of the Configuration Control section of the organization, should be defined and documented throughout the system life cycle of the system under review.

NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, published in August 2011, provides organizations and assessors with many areas of focus and guidance for security CM actions and activities. It starts out by saying: "An information system is composed of many components4 that can be interconnected in a multitude of arrangements to meet a variety of business, mission, and information security ds. How these information system components are networked, configured, and managed is critical in providing adequate information security and supporting an organization's risk management process.

An information system is typically in a constant state of change in response to new, enhanced, corrected, or updated hardware and software capabilities, patches for correcting software flaws and other errors to existing components, new security threats, changing

[4]SP 800-50, p. 8–10.

business functions, etc. Implementing information system changes almost always results in some adjustment to the system configuration. To ensure that the required adjustments to the system configuration do not adversely affect the security of the information system or the organization from operation of the information system, a well-defined configuration management process that integrates information security is needed.

Organizations apply configuration management (CM) for establishing baselines and for tracking, controlling, and managing many aspects of business development and operation (e.g., products, services, manufacturing, business processes, and information technology). Organizations with a robust and effective CM process need to consider information security implications with respect to the development and operation of information systems including hardware, software, applications, and documentation. Effective CM of information systems requires the integration of the management of secure configurations into the organizational CM process or processes. For this reason, this document assumes that information security is an integral part of an organization's overall CM process; however, the focus of this document is on implementation of the information system security aspects of CM, and as such the term *security-focused configuration management* (SecCM) is used to emphasize the concentration on information security. Though both IT business application functions and security-focused practices are expected to be integrated as a single process, *SecCM* in this context is defined as the management and control of configurations for information systems to enable security and facilitate the management of information security risk."[5]

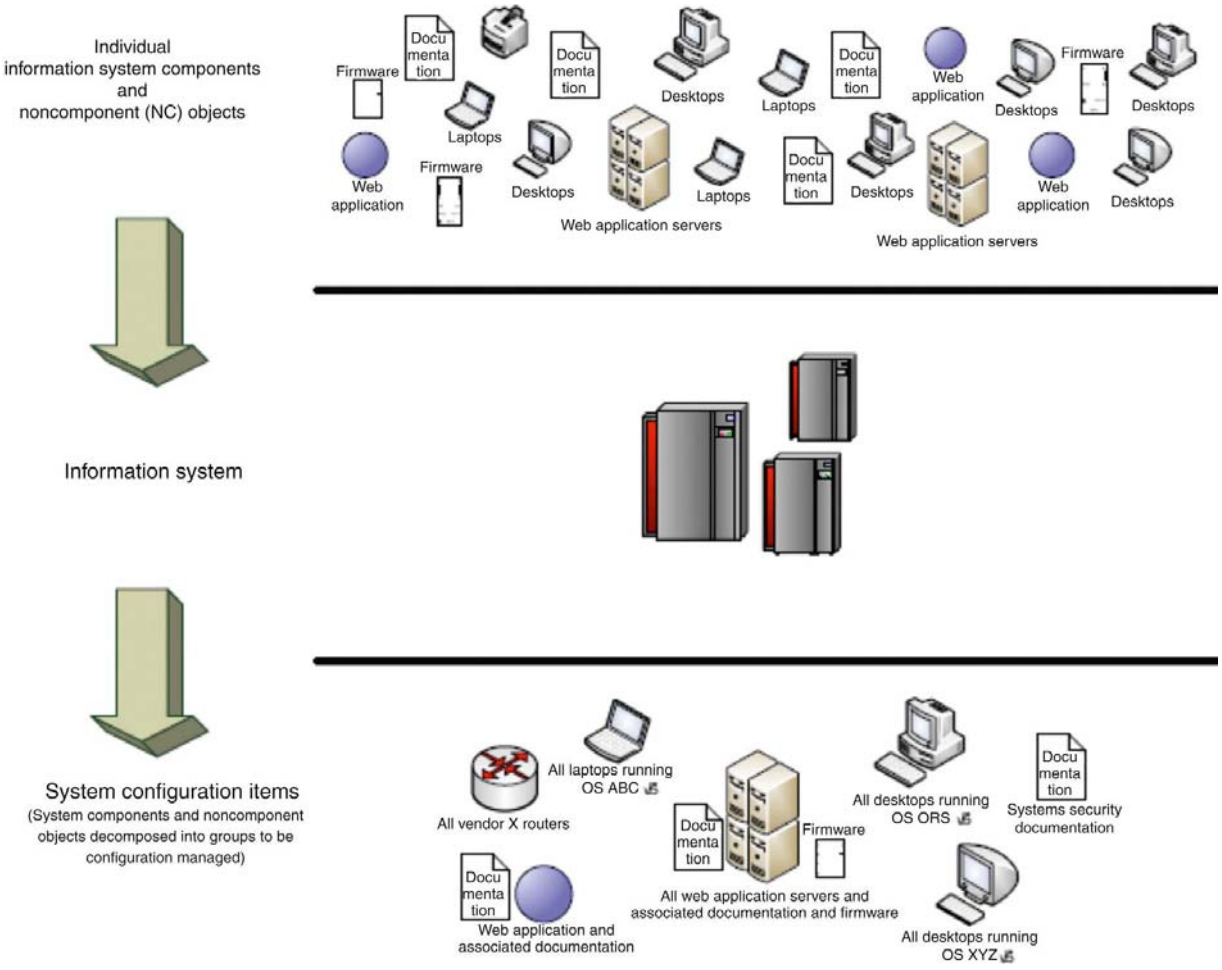
Configuration management has been applied to a broad range of products and systems in subject areas such as automobiles, pharmaceuticals, and information systems. Some basic terms associated with the configuration management discipline are briefly explained below.

- *Configuration Management* (CM) comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.
- A *Configuration Item (CI)* is an identifiable part of a system (e.g., hardware, software, firmware, documentation, or a combination thereof) that is a discrete target of configuration control processes.
- A *Baseline Configuration* is a set of specifications for a system, or CI within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
- A *Configuration Management Plan* (CM Plan) is a comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems. The basic parts of a CM Plan include:
- *Configuration Control Board (CCB)* – Establishment of and charter for a group of qualified people with responsibility for the process of controlling and approving changes throughout the development and operational lifecycle of products and systems; may also be referred to as a change control board;
- Configuration Item *Identification* – methodology for selecting and naming configuration items that need to be placed under CM;
- Configuration *Change Control* – process for managing updates to the baseline configurations for the configuration items; and
- Configuration *Monitoring* – process for assessing or testing the level of compliance with the established baseline configuration and mechanisms for reporting on the configuration status of items placed under CM.

The configuration of an information system is a representation of the system's components, how each component is configured, and how the components are connected or arranged to implement the information

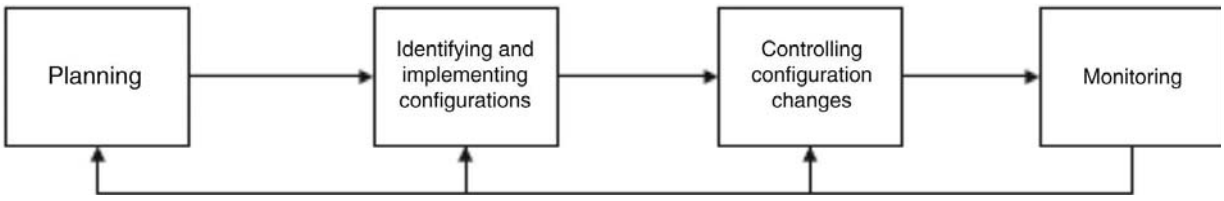
[5]SP 800-128, p. 1.

system. The possible conditions in which an information system or system component can be arranged affect the security posture of the information system. The activities involved in managing the configuration of an information system include development of a configuration management plan, establishment of a configuration control board, development of a methodology for configuration item identification, establishment of the baseline configuration, development of a configuration change control process, and development of a process for configuration monitoring and reporting.[6]



The Phases of Security-Focused Configuration Management

Here are the four defined steps for security CM as found in SP 800-128:



[6]SP 800-128, p. 5–6.

A. **Planning** As a part of planning, the scope or applicability of SecCM processes are identified. Planning includes developing policy and procedures to incorporate SecCM into existing information technology and security programs, and then disseminating the policy throughout the organization. Policy addresses areas such as the implementation of SecCM plans, integration into existing security program plans, Configuration Control Boards (CCBs), configuration change control processes, tools and technology, the use of common secure configurations (A common secure configuration is a recognized, standardized, and established benchmark (e.g., National Checklist Program, DISA STIGs, etc.) that stipulates specific secure configuration settings for a given IT platform.) and baseline configurations, monitoring, and metrics for compliance with established SecCM policy and procedures. It is typically more cost-effective to develop and implement a SecCM plan, policies, procedures, and associated SecCM tools at the organizational level.

B. **Identifying & Implementing Configurations** After the planning and preparation activities are completed, a secure baseline configuration for the information system is developed, reviewed, approved, and implemented. The approved baseline configuration for an information system and associated components represents the most secure state consistent with operational requirements and constraints. For a typical information system, the secure baseline may address configuration settings, software loads, patch levels, how the information system is physically or logically arranged, how various security controls are implemented, and documentation. Where possible, automation is used to enable interoperability of tools and uniformity of baseline configurations across the information system.

C. **Controlling Configuration Changes** In this phase of SecCM, the emphasis is put on the management of change to maintain the secure, approved baseline of the information system. Through the use of SecCM practices, organizations ensure that changes are formally identified, proposed, reviewed, analyzed for security impact, tested, and approved prior to implementation. As part of the configuration change control effort, organizations can employ a variety of access restrictions for change including access controls, process automation, abstract layers, change windows, and verification and audit activities to limit unauthorized and/or undocumented changes to the information system.

D. **Monitoring** Monitoring activities are used as the mechanism within SecCM to validate that the information system is adhering to organizational policies, procedures, and the approved secure baseline configuration. Planning and implementing secure configurations and then controlling configuration change is usually not sufficient to ensure that an information system which was once secure will remain secure. Monitoring identifies undiscovered/undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes, all of which, if not addressed, can expose organizations to increased risk. Using automated tools helps organizations to efficiently identify when the information system is not consistent with the approved baseline configuration and when remediation actions are necessary. In addition, the use of automated tools often facilitates situational awareness and the documentation of deviations from the baseline configuration.[7]

Each area of CM is addressed and covered by security controls identified in SP 800-53 CM family of controls. These areas for assessor focus include:

1. CM Policy and Procedures – CM 1
2. CM Plan – CM 1 and CM 9
3. Configuration Control Board – CM 3
4. Component Inventory – CM 8
5. Configuration Items – CM 3
6. Secure Configurations – CM 6 and CM 7
7. Minimum Security Baseline Configuration – CM 2
8. Configuration Change Control – CM 3 and CM 5
9. Security Impact Analysis – CM 4
10. Configuration Monitoring – all CM controls

[7]SP 800-128, p. 8–9.

Additional guidance for inventory identification and management is also provided in the NIST Interagency Report – NISTIR 7693, *Specifications for Asset Identification*.

Contingency Planning

Information systems are vital elements in most mission/business processes. Because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. CP supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption. It is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level.

Evaluating a recovery and preparedness process for a system, an organization or an application can involve many areas of technology, operations, and the personnel identified throughout an organization. There are many focal points of concern which require analysis and attention of the assessor. As the major area for the controls related to the security objective of availability, CP has become a focal point for assessors to determine the commitment of the organization's senior management to the security of their operational systems and applications.

Under Federal Continuity Directive (FCD)-1 and FCD-2 all federal information systems require a contingency plan for recovery and restoration efforts. Additional guidance is provided by NIST is SP 800-34 and templates available on the csrc.nist.gov website.

Information system CP represents a broad scope of activities designed to sustain and recover critical system services following an emergency event. Information system CP fits into a much broader security and emergency management effort that includes organizational and business process continuity, disaster recovery planning, and incident management. Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's information systems, mission/business processes, personnel, and the facility. Because there is an inherent relationship between an information system and the mission/business process it supports, there must be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

> Continuity and contingency planning are critical components of emergency management and organizational resilience but are often confused in their use. *Continuity planning* normally applies to the mission/business itself; it concerns the ability to continue critical functions and processes during and after an emergency event. *Contingency planning* normally applies to information systems, and provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency. *Cyber Incident Response Planning* is a type of plan that normally focuses on detection, response, and recovery to a computer security incident or event.[8]

[8]SP 800-34, p. 7.

Contingency-related plan relationships

Details for each type of plan and its development, use, and maintenance are found in SP 800-34.

The primary focus of each plan is listed as follows:

Plan	Purpose	Scope	Plan relationship
Business Continuity Plan (BCP)	Provides procedures for sustaining mission/ business operations while recovering from a significant disruption	Addresses mission/ business processes at a lower or expanded level from Continuity of Operations (COOP) MEFs	Mission/business process focused plan that may be activated in coordination with a COOP plan to sustain non-MEFs
COOP Plan	Provides procedures and guidance to sustain an organization's Metro Ethernet Forums (MEFs) at an alternate site for up to 30 days; mandated by federal directives	Addresses MEFs at a facility; information systems are addressed based only on their support of the mission essential functions	MEF focused plan that may also activate several business unit-level BCPs, Information System Contingency Plans (ISCPs), or Disaster Recovery Plans (DRPs), as appropriate
Crisis Communications Plan	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors	Addresses communications with personnel and the public; not information system-focused	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event

(*Continued*)

Plan	Purpose	Scope	Plan relationship
Critical Infrastructure Protection (CIP) Plan	Provides policies and procedures for protection of national critical infrastructure components, as defined in the National Infrastructure Protection Plan	Addresses critical infrastructure components that are supported or operated by an agency or organization	Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets
Cyber Incident Response Plan	Provides procedures for mitigating and correcting a cyber attack, such as a virus, worm, or Trojan horse	Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information	Information system-focused plan that may activate an ISCP or DRP, depending on the extent of the attack
DRP	Provides procedures for relocating information systems operations to an alternate location	Activated after major system disruptions with long-term effects	Information system-focused plan that activates one or more ISCPs for recovery of individual systems
ISCP	Provides procedures and capabilities for recovering an information system	Addresses single information system recovery at the current or, if appropriate, alternate location	Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP. COOP, and/or BCP
Occupant Emergency Plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat	Focuses on personnel and property particular to the specific facility: not mission/business process or information system-based	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation

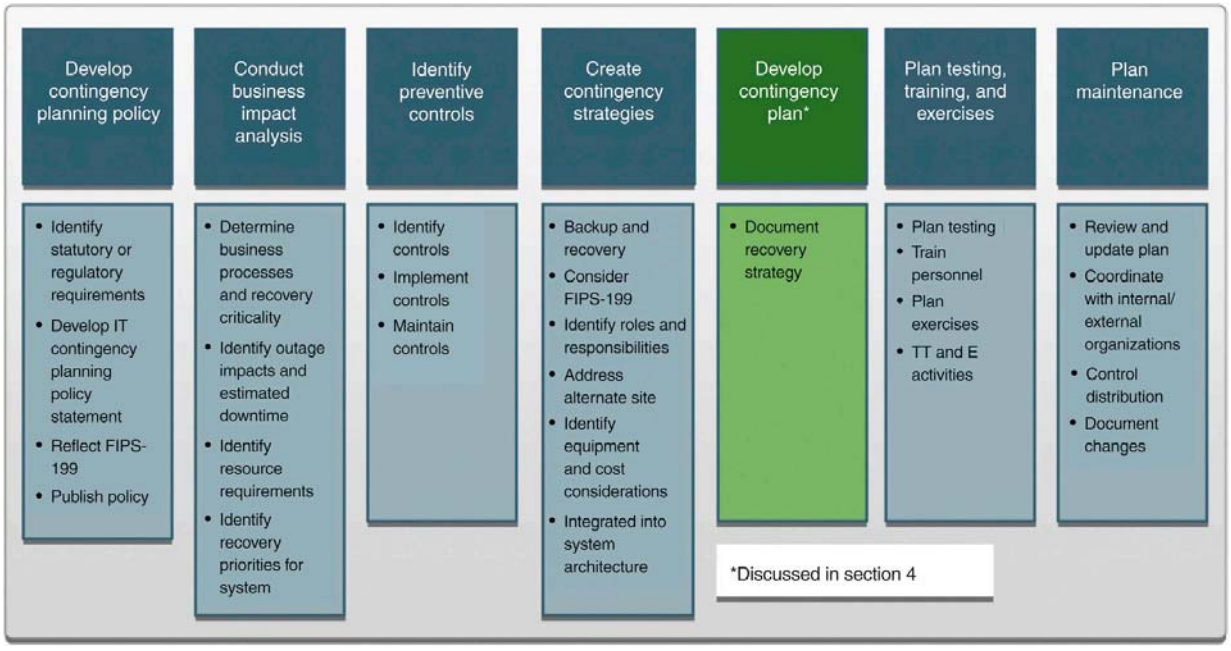
Seven Steps to Contingency Planning as Defined in SP 800-34

SP 800-34, rev. 1, provides instructions, recommendations, and considerations for federal information system CP. CP refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods. This guide addresses specific CP recommendations for three platform types and provides strategies and techniques common to all systems:

- Client/server systems
- Telecommunications systems
- Mainframe systems

This guide defines the following seven-step CP process that an organization may apply to develop and maintain a viable CP program for their information systems. These seven progressive steps are designed to be integrated into each stage of the system development life cycle:

1. *Develop the CP policy statement.* A formal policy provides the authority and guidance necessary to develop an effective contingency plan.
2. *Conduct the business impact analysis (BIA).* The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business processes.
3. *Identify preventive controls.* Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life-cycle costs.
4. *Create contingency strategies.* Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
5. *Develop an information system contingency plan.* The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.
6. *Ensure plan testing, training, and exercises.* Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.
7. *Ensure plan maintenance.* The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.



The assessor should be looking for multiple areas of focus which the organization has applied in its CP activities. SP 800-34 provides the agencies and organizations the guidance to conduct these events and the assessor gathers the evidence to ensure these events have been conducted in accordance with these guidelines.

Key points to review and assess include:

1. The CP policy statement:
   a. Policy should define the organization's overall contingency objectives and establish the organizational framework and responsibilities for system CP.
   b. To be successful, senior management, most likely the CIO, must support a contingency program and be included in the process to develop the program policy.
   c. The policy must reflect the FIPS-199 impact levels and the contingency controls that each impact level establishes. Key policy elements are as follows:
      - Roles and responsibilities
      - Scope as applies to common platform types and organization functions (i.e., telecommunications, legal, media relations) subject to CP
      - Resource requirements
      - Training requirements
      - Exercise and testing schedules
      - Plan maintenance schedule
      - Minimum frequency of backups and storage of backup media
2. The ISCPs must be written in coordination with other plans associated with each target system as part of organization-wide resilience strategy. Such plans include the following:
   a. Information SSPs
   b. Facility-level plans, such as the OEP and DRP
   c. MEF support such as the COOP plan
   d. Organization-level plans, such as CIP plans

BIA Requirements

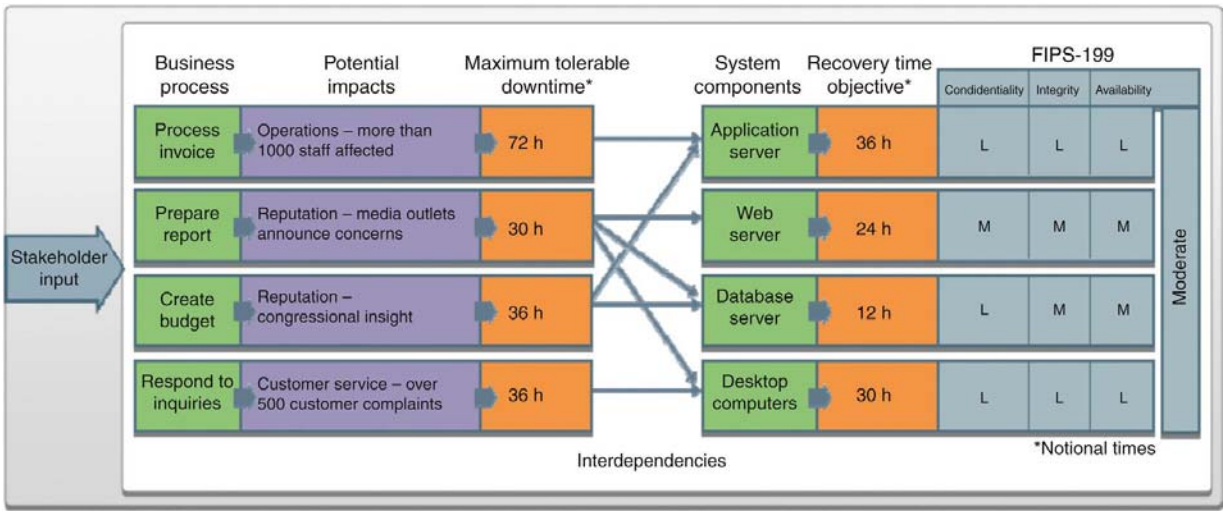
The BIA purpose is to correlate the system with the critical mission/business processes and services provided, and based on that information, characterize the consequences of a disruption. The ISCP Coordinator can use the BIA results to determine contingency planning requirements and priorities. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's COOP, BCPs, and DRP.

Three steps are typically involved in accomplishing the BIA:

1. **Determine mission/business processes and recovery criticality.** Mission/Business processes supported by the system are identified and the impact of a system disruption to those processes is determined **along with outage impacts and estimated downtime.** The downtime should reflect the maximum time that an organization can tolerate while still maintaining the mission.
2. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
3. **Identify recovery priorities for system resources.** Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources.

The sample BIA process and data collection activities, outlined in this section and illustrated below, consisting of a representative information system with multiple components (servers), are designed to help the ISCP Coordinator streamline and focus contingency plan development activities to achieve a more effective plan.[9]

[9]SP 800-34, p. 15–16.



Numbers that Matter – Critical Recovery Numbers

The assessor always needs to keep the numbers that matter to the business objectives and mission when reviewing the CP and COOP documentation, evidence, and testing results. So, what are these numbers?

- Maximum tolerable downtime (MTD)
- Recovery time objective (RTO)
- Recovery point objective (RPO)

The ISCP Coordinator should next analyze the supported mission/business processes and with the process owners, leadership and business managers determine the acceptable downtime if a given process or specific system data were disrupted or otherwise unavailable. Downtime can be identified in several ways.

- **Maximum Tolerable Downtime (MTD).** The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.
- **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD. When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Action and Milestone should be initiated to document the situation and plan for its mitigation.
- **Recovery Point Objective (RPO**). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process.

Because the RTO must ensure that the MTD is not exceeded, the RTO must normally be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.[10]

[10]SP 800-34, p. 17.

Example:

COOP VERSUS ISCP – THE BASIC FACTS

Recovery times

- COOP functions must be sustained within 12 h and for up to 30 days from an alternate site; ISCP RTOs are determined by the system-based BIA.
  - Information systems that support COOP functions must have an RTO that meets COOP requirements.
  - Information systems that do not support COOP functions do not *require* alternate sites as part of the ISCP recovery strategy, but may have an alternate site security control requirement.

Recovery Strategies

FIPS-199 availability impact level	Information system target priority and recovery	Backup/recovery strategy
Low	Low priority – any outage with little impact, damage, or disruption to the organization	*Backup*: Tape backup *Strategy*: Relocate or cold site
Moderate	Important or moderate priority – any system that, if disrupted, would cause a moderate problem to the organization and possibly other networks or systems	*Backup*: Optical backup. WAN/VLAN replication *Strategy*: Cold or warm site
High	Mission-critical or high priority – the damage or disruption to these systems would cause the most impact on the organization, mission, and other networks and systems	*Backup*: Mirrored systems and disc replication *Strategy*: Hot site

Site	Cost	Hardware equipment	Telecommunications	Setup time	Location
Cold site	Low	None	None	Long	Fixed
Warm site	Medium	Partial	Partial/full	Medium	Fixed
Hot site	Medium/high	Full	Full	Short	Fixed

As an assessor, the job here is to evaluate and assess whether the numbers identified above do three things:

1. Provide the appropriate level of recovery in relation to the security categorization of the system under review

2. Provide the level of recovery expected and documented in the BIA for the system under review
3. Provide the level of recovery expected by the end using organization and their financial commitment

The various recovery processes and procedures need to be verified and validated, which is typically done through the use of testing and exercises conducted in accordance with SP 800-82.

SP 800-82, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

Organizations have IT plans in place, such as contingency and computer security IR plans, so that they can respond to and manage adverse situations involving IT. These plans should be maintained in a state of readiness, which should include having personnel trained to fulfill their roles and responsibilities within a plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in an operational environment specified in a plan. These three types of events can be carried out efficiently and effectively through the development and implementation of a test, training, and exercise (TT&E) program. Organizations should consider having such a program in place because tests, training, and exercises are so closely related. For example, exercises and tests offer different ways of identifying deficiencies in IT plans, procedures, and training.[11]

TEST

Tests are evaluation tools that use quantifiable metrics to validate the operability of an IT system or system component in an operational environment specified in an IT plan. For example, an organization could test if call tree cascades can be executed within prescribed time limits; another test would be removing power from a system or system component. A test is conducted in as close to an operational environment as possible; if feasible, an actual test of the components or systems used to conduct daily operations for the organization should be used. The scope of testing can range from individual system components or systems to comprehensive tests of all systems and components that support an IT plan. Tests often focus on recovery and backup operations; however, testing varies depending on the goal of the test and its relation to a specific IT plan.

TRAINING

Training, in this recovery context, refers only to informing personnel of their roles and responsibilities within a particular IT plan and teaching them skills related to those roles and responsibilities, thereby preparing them for participation in exercises, tests, and actual emergency situations related to the IT plan. Training personnel on their roles and responsibilities before an exercise or test event is typically split between a presentation on their roles and responsibilities and activities that allow personnel to demonstrate their understanding of the subject matter.

EXERCISES

An exercise is a simulation of an emergency designed to validate the viability of one or more aspects of an IT plan. In an exercise, personnel with roles and responsibilities in a

[11]SP 800-82, p. ES-1.

particular IT plan meet to validate the content of a plan through discussion of their roles and their responses to emergency situations, execution of responses in a simulated operational environment, or other means of validating responses that does not involve using the actual operational environment. Exercises are scenario-driven, such as a power failure in one of the organization's data centers or a fire causing certain systems to be damaged, with additional situations often being presented during the course of an exercise. There are several types of exercises, and this publication focuses on the following two types that are widely used in TT&E programs by single organizations:

- *Tabletop*: Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.
- *Functional*: Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. They are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, IT equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. They allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner.

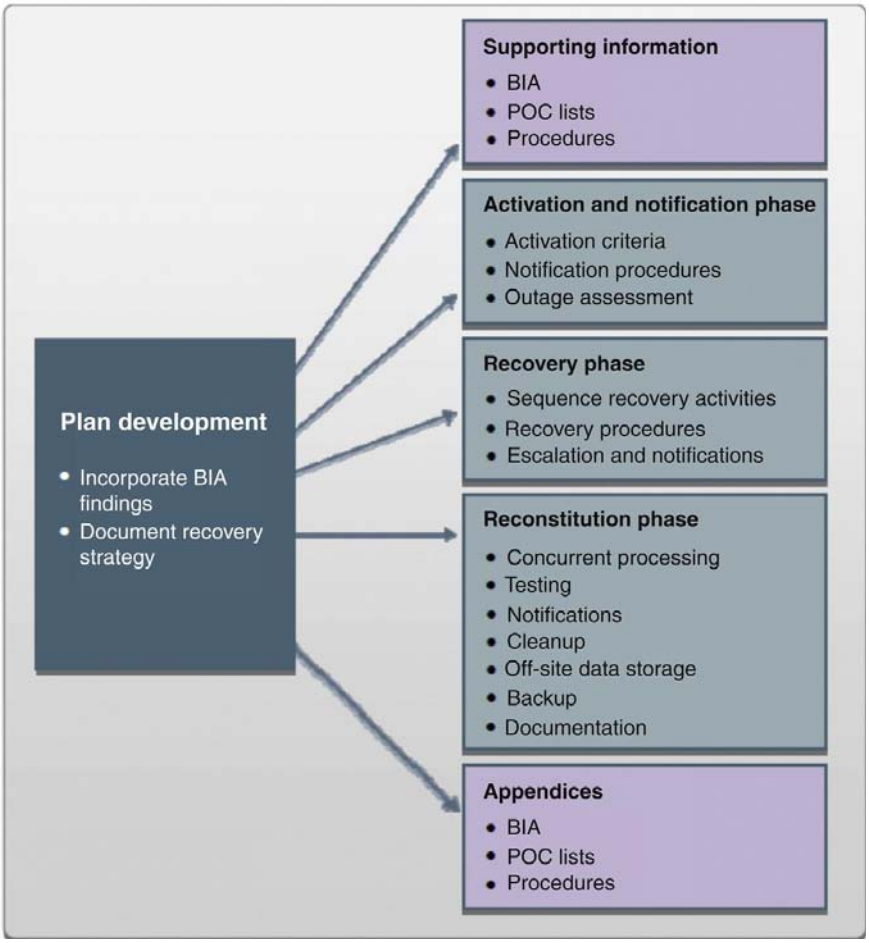
Contingency Plan Testing

Contingency plan testing always requires special attention for assessors as this is often the only way to fully check out the alternative operations and support efforts that the organization has placed into operations but only activates when they are required to do so. The following table reflects the areas of CP controls to evaluate and obtain evidence and proof of accomplishment for testing of the various parts of the system or organization's contingency plans and COOP preparations:

Control	Testing event	Sample event to document
CP-3	CP training	A seminar and/or briefing used to familiarize personnel with the overall CP purpose, phases, activities, and roles and responsibilities
CP-3	Instruction	Instruction of contingency personnel on their roles and responsibilities within the CP and includes refresher training and, for high-impact systems, simulated events
CP-4	CP testing/exercise	Test and/or exercise the CP to determine the effectiveness and the organization's readiness. This includes both planned and unplanned maintenance activities
CP-4	Tabletop exercise	Discussion-based simulation of an emergency-based situation in an informal stress-free environment; designed to elicit constructive scenario-based discussions for an examination of the existing CP and individual state of preparedness

Control	Testing event	Sample event to document
CP-4	Functional exercise	Simulation of a disruption with a system recovery component such as backup tape restoration or server recovery
CP-4	Full-scale functional exercise	Simulation prompting a full recovery and reconstitution of the information system to a known state and ensures that staff are familiar with the alternative facility
CP-4, CP-7	Alternate processing site recovery	Test and/or exercise the CP at the alternate processing site to familiarize contingency personnel with the facility and available resources and evaluate the site's capabilities to support contingency operations. Includes a full recovery and return to normal operations to a known secure state. If high-impact system, the alternate facility should be fully configured as defined in CP
CP-9	System backup	Test backup information to verify media reliability and information integrity. If high-impact system, use sample backup information to validate recovery process and ensure backup copies are maintained at alternate storage facility

Now, each of these areas of focus for assessment of the CP controls should be tied into and reflected in the system contingency plan and its design efforts as reflected in the following:



Incident Response

The current state of the security of systems across the enterprise often requires organizations to develop and conduct IR activities due to breaches, malware infections, "phishing" events, and outright external attacks. The state of the cybercrime and hacking communities has developed dramatically over the past few years and now includes "hack-in-a-box" and fully developed malicious software development efforts including formal version controls, automated delivery channels, testing against known antivirus signatures, and malware as a service (MAAS) cloud-based delivery mechanisms. The goals of any IR effort are as follows:

- Detect incidents quickly.
- Diagnose incidents accurately.
- Manage incidents properly.
- Contain and minimize damage.
- Restore affected services.
- Determine root causes.
- Implement improvements to prevent recurrence.
- Document and report.

The purpose of IR is to manage and respond to unexpected disruptive events with the objective of controlling impacts within acceptable levels. These events can be technical, such as attacks mounted on the network via viruses, denial of service, or system intrusion, or they can be the result of mistakes, accidents, or system or process failure. Disruptions can also be caused by a variety of physical events such as theft of proprietary information, social engineering, lost or stolen backup tapes or laptops, environmental conditions such as floods, fires, or earthquakes, and so forth. Any type of incident that can significantly affect the organization's ability to operate or that may cause damage must be considered by the information security manager and will normally be a part of incident management and response capabilities.

The US government has long recognized the need and requirements for computer IR and, as a result, has developed many documented resources and organizations for IR to include the US-Computer Emergency Response Team (CERT), various DOD CERT organizations, joint ventures between various governmental agencies, incident handling guides, procedures and techniques, and the NIST SP 800-61.

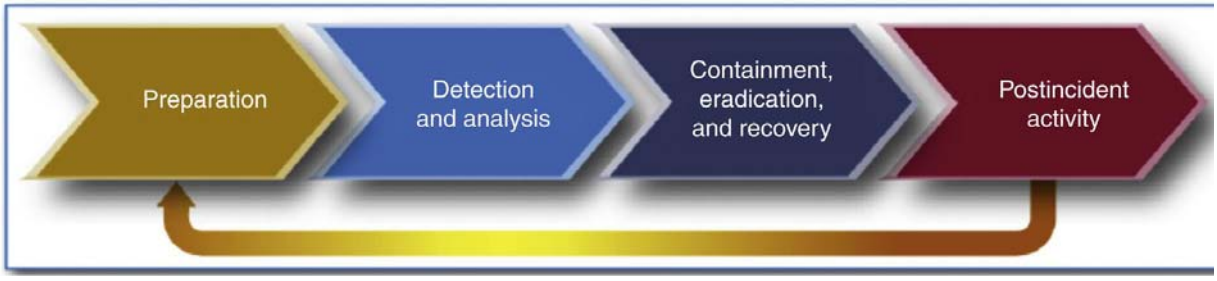
SP 800-61 – Computer Security Incident Handling Guide

As the introduction at the beginning of SP 800-61 says: "Computer security incident response has become an important component of information technology (IT) programs. Cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services. To that end, this publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications.

Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. Continually monitoring for attacks is essential. Establishing clear procedures for prioritizing the handling of incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data. It is also vital to build relationships and establish suitable means of communication with other internal groups (e.g., human resources, legal) and with external groups (e.g., other incident response teams, law enforcement)."[12]

Incident Handling

> The incident response process has several phases. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, the organization also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. However, residual risk will inevitably persist after controls are implemented. Detection of security breaches is thus necessary to alert the organization whenever incidents occur. In keeping with the severity of the incident, the organization can mitigate the impact of the incident by containing it and ultimately recovering from it. During this phase, activity often cycles back to detection and analysis—for example, to see if additional hosts are infected by malware while eradicating a malware incident. After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents.[13]



PREPARATION

IR methodologies typically emphasize preparation – not only establishing an IR capability so that the organization is ready to respond to incidents but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Although the IR team is not typically responsible for incident prevention, it is fundamental to the success of IR programs.

As an assessor of IR capacity and incident handling activities, it is important to understand the process itself is often chaotic and can appear haphazard when the response is active. One of the critical areas to focus on during the review is the documented and defined training for the responders, as well as the organizational policies and procedures for IR. Each of these areas helps determine the success or failure of the response team, their interactions with the rest of the organization, and ultimately the minimization of the impact of the incident on the organization, its people, and its mission.

[12]SP 800-61, rev. 2, p. 1.
[13]*Ibid.*, p. 21.

DETECTION AND ANALYSIS

For many organizations, the most challenging part of the incident response process is accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem. What makes this so challenging is a combination of three factors:

- Incidents may be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include network-based and host-based IDPSs, antivirus software, and log analyzers. Incidents may also be detected through manual means, such as problems reported by users. Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect.
- The volume of potential signs of incidents is typically high—for example, it is not uncommon for an organization to receive thousands or even millions of intrusion detection sensor alerts per day.
- Deep, specialized technical knowledge and extensive experience are necessary for proper and efficient analysis of incident-related data.

Signs of an incident fall into one of two categories: precursors and indicators. A *precursor* is a sign that an incident may occur in the future. An *indicator* is a sign that an incident may have occurred or may be occurring now.

Incident detection and analysis would be easy if every precursor or indicator were guaranteed to be accurate; unfortunately, this is not the case. For example, user-provided indicators such as a complaint of a server being unavailable are often incorrect. Intrusion detection systems may produce false positives—incorrect indicators. These examples demonstrate what makes incident detection and analysis so difficult: each indicator ideally should be evaluated to determine if it is legitimate. Making matters worse, the total number of indicators may be thousands or millions a day. Finding the real security incidents that occurred out of all the indicators can be a daunting task.

Even if an indicator is accurate, it does not necessarily mean that an incident has occurred. Some indicators, such as a server crash or modification of critical files, could happen for several reasons other than a security incident, including human error. Given the occurrence of indicators, however, it is reasonable to suspect that an incident might be occurring and to act accordingly. Determining whether a particular event is actually an incident is sometimes a matter of judgment. It may be necessary to collaborate with other technical and information security personnel to make a decision. In many instances, a situation should be handled the same way regardless of whether it is security related. For example, if an organization is losing Internet connectivity every 12 hours and no one knows the cause, the staff would want to resolve the problem just as quickly and would use the same resources to diagnose the problem, regardless of its cause.[14]

CONTAINMENT, ERADICATION, AND RECOVERY

Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision making (e.g., shut down a system, disconnect it from a network, or disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident. Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly.

Containment strategies vary based on the type of incident. For example, the strategy for containing an email-borne malware infection is quite different from that for a network-based DDoS attack. Organizations should create separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision making.[15]

[14]SP 800-61, rev. 2, p. 25, 28.

[15]SP 800-61, rev. 2, p. 35.

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists). Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner.

Eradication and recovery should be done in a phased approach so that remediation steps are prioritized. For large-scale incidents, recovery may take months; the intent of the early phases should be to increase the overall security with relatively quick (days to weeks) high value changes to prevent future incidents. The later phases should focus on longer-term changes (e.g., infrastructure changes) and ongoing work to keep the enterprise as secure as possible.[16]

POSTINCIDENT ACTIVITY

One of the most important parts of incident response is also the most often omitted: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned. Holding a "lessons learned" meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself. Multiple incidents can be covered in a single lessons learned meeting. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked.

Small incidents need limited post-incident analysis, with the exception of incidents performed through new attack methods that are of widespread concern and interest. After serious attacks have occurred, it is usually worthwhile to hold post-mortem meetings that cross team and organizational boundaries to provide a mechanism for information sharing. The primary consideration in holding such meetings is ensuring that the right people are involved. Not only is it important to invite people who have been involved in the incident that is being analyzed, but also it is wise to consider who should be invited for the purpose of facilitating future cooperation.[17]

As an IR assessor and evaluator, you will be looking for the required training and exercise documentation for each responder on the team. The policies for IR, handling, notification, and board review all need to be identified, reviewed, and assessed. The supporting procedures for handling and response efforts all need review and correlation to the policies, the security controls for IR from SP 800-53 and the actual IR plan for each system as it is reviewed and assessed.

Federal Agency Incident Categories

To clearly communicate incidents and events (any observable occurrence in a network or system) throughout the Federal Government and supported organizations, it is necessary for the government incident response teams to adopt a common set of terms and relationships between those terms. All elements of the Federal Government should use a common taxonomy.

Below please find a high level set of concepts and descriptions to enable improved communications among and between agencies. The taxonomy below does not replace discipline (technical, operational, intelligence) that needs to occur to defend federal agency computers/networks, but provides a common platform to execute the US-CERT mission. US-CERT and the federal civilian agencies are to utilize the following incident and event categories and reporting timeframe criteria as the federal agency reporting taxonomy.

[16]SP 800-61, rev. 2, p. 37.

[17]SP 800-61, rev. 2, p. 38–39.

Federal Agency Incident Categories

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resources	Within one (1) hour of discovery/detection
CAT 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	Malicious Code	*Successful* installation of malicious software (e.g., virus, worm. Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes/ Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

- CAT 0 - Exercise/Network Defense Testing
- CAT 1 - *Unauthorized Access
- CAT 2 - *Denial of Service (DoS)
- CAT 3 - *Malicious Code
- CAT 4 - *Inappropriate Usage
- CAT 5 - Scans/Probes/Attempted Access
- CAT 6 – Investigation

***Any incident that involves compromised PII must be reported to US-CERT within 1 hour of detection regardless of the incident category reporting timeframe.**[18]

Now, as of October 1, 2014 US-CERT posted a new taxonomy and methodology for reporting of incidents. US-CERT posted the following information and table for the new requirements, which are required to be used after September 1, 2015:

> Please use the table below to identify the impact of the incident. Incidents may affect multiple types of data; therefore, D/As may select multiple options when identifying the information impact. The security categorization of federal information and information systems must be determined in accordance with Federal Information Processing Standards (FIPS) Publication 199. Specific thresholds for loss of service availability (i.e., all, subset, loss of efficiency) must be defined by the reporting organization.[19]

Impact Classifications	Impact Description
Functional Impact	**HIGH** - Organization has lost the ability to provide all critical services to all system users.
	MEDIUM - Organization has lost the ability to provide a critical service to a subset of system users.
	LOW - Organization has experienced a loss of efficiency, but can still provide all critical services to all users with minimal effect on performance.
	NONE - Organization has experienced no loss in ability to provide all services to all users.
Information Impact	**CLASSIFIED** - The confidentiality of classified information [5] was compromised.
	PROPRIETARY [6] - The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.
	PRIVACY - The confidentiality of personally identifiable information [7] (PII) of personal health information (PHI) was compromised.
	INTEGRITY - The necessary integrity of information was modified without authorization.
	NONE - No information was exfiltrated. modified, deleted, or otherwise compromised.
Recoverability	**REGULAR** - Time to recovery is predictable with existing resources.
	SUPPLEMENTED - Time to recovery is predictable with additional resources.
	EXTENDED - Time to recovery is unpredictable; additional resources and outside help are needed.
	NOT RECOVERABLE - Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).
	NOT APPLICABLE - Incident does not require recovery.

To minimize damage from security incidents and to recover and to learn from such incidents, a formal IR capability should be established. The organization and management of an IR capability should be coordinated or centralized with the establishment of key roles and responsibilities. In establishing this process, employees and contractors are made aware of procedures for reporting the different types of incidents that might have an impact on the security of organizational assets. Incidents occur because vulnerabilities are not addressed

[18]https://www.us-cert.gov/government-users/reporting-requirements, retrieved 2/1/2015.

[19]https://www.us-cert.gov/incident-notification-guidelines, retrieved 2/1/2015.

properly. Ideally, an organizational computer security incident response team (CSIRT) or CERT should be formulated with clear lines of reporting, and responsibilities for standby support should be established. An assessor should ensure that the CSIRT is actively involved with users to assist them in the mitigation of risks arising from security failures and also to prevent security incidents.

The assessor needs to check for, evaluate, and assess the following areas of IR:

A. **Organizations must create, provision, and operate a formal incident response capability. Federal law requires Federal agencies to report incidents to the United States Computer Emergency Readiness Team (US-CERT) office within the Department of Homeland Security (DHS).**
The Federal Information Security Management Act (FISMA) requires Federal agencies to establish incident response capabilities. Each Federal civilian agency must designate a primary and secondary point of contact (POC) with US-CERT and report all incidents consistent with the agency's incident response policy. Each agency is responsible for determining how to fulfill these requirements. Establishing an incident response capability should include the following actions:

1. Creating an incident response policy and plan
2. Developing procedures for performing incident handling and reporting
3. Setting guidelines for communicating with outside parties regarding incidents
4. Selecting a team structure and staffing model
5. Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)
6. Determining what services the incident response team should provide
7. Staffing and training the incident response team.

B. **Organizations should reduce the frequency of incidents by effectively securing networks, systems, and applications.**
Preventing problems is often less costly and more effective than reacting to them after they occur. Thus, incident prevention is an important complement to an incident response capability. If security controls are insufficient, high volumes of incidents may occur. This could overwhelm the resources and capacity for response, which would result in delayed or incomplete recovery and possibly more extensive damage and longer periods of service and data unavailability. Incident handling can be performed more effectively if organizations complement their incident response capability with adequate resources to actively maintain the security of networks, systems, and applications. This includes training IT staff on complying with the organization's security standards and making users aware of policies and procedures regarding appropriate use of networks, systems, and applications.

C. **Organizations should document their guidelines for interactions with other organizations regarding incidents.**
During incident handling, the organization will need to communicate with outside parties, such as other incident response teams, law enforcement, the media, vendors, and victim organizations. Because these communications often need to occur quickly, organizations should predetermine communication guidelines so that only the appropriate information is shared with the right parties.

D. **Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors.**
Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident. This publication defines several types of incidents, based on common attack vectors; these categories are not intended to provide definitive classification for incidents, but rather to be used as a basis for defining more specific handling procedures. Different types of incidents merit different response strategies. The attack vectors are:

- **External/Removable Media:** An attack executed from removable media (e.g., flash drive, CD) or a peripheral device.
- **Attrition:** An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.

- **Web:** An attack executed from a website or web-based application.
- **Email:** An attack executed via an email message or attachment.
- **Improper Usage:** Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.
- **Loss or Theft of Equipment:** The loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.
- **Other:** An attack that does not fit into any of the other categories.

E. **Organizations should emphasize the importance of incident detection and analysis throughout the organization.**
In an organization, millions of possible signs of incidents may occur each day, recorded mainly by logging and computer security software. Automation is needed to perform an initial analysis of the data and select events of interest for human review. Event correlation software can be of great value in automating the analysis process. However, the effectiveness of the process depends on the quality of the data that goes into it. Organizations should establish logging standards and procedures to ensure that adequate information is collected by logs and security software and that the data is reviewed regularly.

F. **Organizations should create written guidelines for prioritizing incidents.**
Prioritizing the handling of individual incidents is a critical decision point in the incident response process. Effective information sharing can help an organization identify situations that are of greater severity and demand immediate attention. Incidents should be prioritized based on the relevant factors, such as the functional impact of the incident (e.g., current and likely future negative impact to business functions), the information impact of the incident (e.g., effect on the confidentiality, integrity, and availability of the organization's information), and the recoverability from the incident (e.g., the time and types of resources that must be spent on recovering from the incident).

G. **Organizations should use the lessons learned process to gain value from incidents.**
After a major incident has been handled, the organization should hold a "lessons learned" meeting to review the effectiveness of the incident handling process and identify necessary improvements to existing security controls and practices. Lessons learned meetings can also be held periodically for lesser incidents as time and resources permit. The information accumulated from all lessons learned meetings should be used to identify and correct systemic weaknesses and deficiencies in policies and procedures. Follow-up reports generated for each resolved incident can be important not only for evidentiary purposes but also for reference in handling future incidents and in training new team members.[20]

System Maintenance

As an assessor of federal information systems, what do you need to know about operations and maintenance (O&M) of information systems?

In the maintenance area for systems, focus on the policies and procedures for the maintenance activities of the assigned personnel first. Then look at the maintenance records, logs, and reports of the maintenance staff. Check these records against the requests and help desk tickets to ensure the maintenance is requested legitimately, performed appropriately, and completed successfully.

Areas for review include the following parts of the Maintenance and Support program of the agency:

- Nonlocal maintenance = remote access/maintenance:
  - FIPS-201-1 Common Identification – Personal Identity Verification (PIV; IA)
  - SP 800-63 e-authentication (IA)
  - FIPS-197 Advance Encryption Standard (systems and communications protection (SC))
  - FIPS-140-2 Cryptography Standard
  - SP 80-88 Media Sanitization (MP)

[20]SP 800-61, rev. 2, p. 2–3.

- Planning for failure of equipment:
  - Mean time between failures (MTBF)
  - Mean time to repair (MTTR)

Encryption Standards for Use and Review in Federal Systems

FIPS-140-1 was developed by a government and industry working group composed of both operators and vendors. The working group identified requirements for four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g., low-value administrative data, million dollar funds transfers, and life-protecting data) and a diversity of application environments (e.g., a guarded facility, an office, and a completely unprotected location). Four security levels are specified for each of 11 requirement areas. Each security level offers an increase in security over the preceding level. These four increasing levels of security allow cost-effective solutions that are appropriate for different degrees of data sensitivity and different application environments. FIPS-140-2 incorporates changes in applicable standards and technology since the development of FIPS-140-1 as well as changes that are based on comments received from the vendor, laboratory, and user communities. The basic level guidance from the FIPS is provided as follows:

1. *Security Level 1*: Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one approved algorithm or approved security function shall be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.

   Security Level 1 allows the software and firmware components of a cryptographic module to be executed on a general-purpose computing system using an unevaluated operating system. Such implementations may be appropriate for some low-level security applications when other controls, such as physical security, network security, and administrative procedures, are limited or nonexistent. The implementation of cryptographic software may be more cost-effective than corresponding hardware-based mechanisms, enabling organizations to select from alternative cryptographic solutions to meet lower-level security requirements.
2. *Security Level 2*: Security Level 2 enhances the physical security mechanisms of a Security Level 1 cryptographic module by adding the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals or for pick-resistant locks on removable covers or doors of the module. Tamper-evident coatings or seals are placed on a cryptographic module so that the coating or seal must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module. Tamper-evident seals or pick-resistant locks are placed on covers or doors to protect against unauthorized physical access.

   Security Level 2 requires, at a minimum, role-based authentication in which a cryptographic module authenticates the authorization of an operator to assume a specific role and perform a corresponding set of services.

   Security Level 2 allows the software and firmware components of a cryptographic module to be executed on a general-purpose computing system using an operating system that:

a. Meets the functional requirements specified in the Common Criteria (CC) Protection Profiles (PPs)
b. Is evaluated at the CC evaluation assurance level EAL2 (or higher)

An equivalent evaluated trusted operating system may be used. A trusted operating system provides a level of trust so that cryptographic modules executing on general-purpose computing platforms are comparable to cryptographic modules implemented using dedicated hardware systems.

3. *Security Level 3*: In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use, or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroizes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.

   Security Level 3 requires identity-based authentication mechanisms, enhancing the security provided by the role-based authentication mechanisms specified for Security Level 2. A cryptographic module authenticates the identity of an operator and verifies that the identified operator is authorized to assume a specific role and perform a corresponding set of services.

   Security Level 3 requires the entry or output of plaintext CSPs (including the entry or output of plaintext CSPs using split knowledge procedures) be performed using ports that are physically separated from other ports, or interfaces that are logically separated using a trusted path from other interfaces. Plaintext CSPs may be entered into or output from the cryptographic module in encrypted form (in which case they may travel through enclosing or intervening systems).

   Security Level 3 allows the software and firmware components of a cryptographic module to be executed on a general-purpose computing system using an operating system that:

   a. Meets the functional requirements specified in the PPs listed in Annex B with the additional functional requirement of a trusted path (FTP_TRP.1)
   b. Is evaluated at the CC evaluation assurance level EAL3 (or higher) with the additional assurance requirement of an informal Target of Evaluation (TOE) Security Policy Model (ADV_SPM.1)

   An equivalent evaluated trusted operating system may be used. The implementation of a trusted path protects plaintext CSPs and the software and firmware components of the cryptographic module from other untrusted software or firmware that may be executing on the system.

4. *Security Level 4*: Security Level 4 provides the highest level of security defined in this standard. At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate zeroization of all plaintext CSPs. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments.

Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges may be used by an attacker to thwart a cryptographic module's defenses. A cryptographic module is required either to include special environmental protection features designed to detect fluctuations and zeroize CSPs or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module.

Security Level 4 allows the software and firmware components of a cryptographic module to be executed on a general-purpose computing system using an operating system that:

a. Meets the functional requirements specified for Security Level 3

b. Is evaluated at the CC evaluation assurance level EAL4 (or higher)

An equivalent evaluated trusted operating system may be used.

5. *Advanced Encryption Standard*: FIPS-197, Advanced Encryption Standard (AES), specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.

The algorithm may be used with the three different key lengths indicated above, and therefore these different "flavors" may be referred to as "AES-128," "AES-192," and "AES-256."

Media Protection

- SP 800-88 – sanitization
- SP 800-111 – storage encryption

Media Sanitation

The information security concern regarding information disposal and media sanitization resides not in the media but in the recorded information. The issue of media disposal and sanitization is driven by the information placed intentionally or unintentionally on the media.

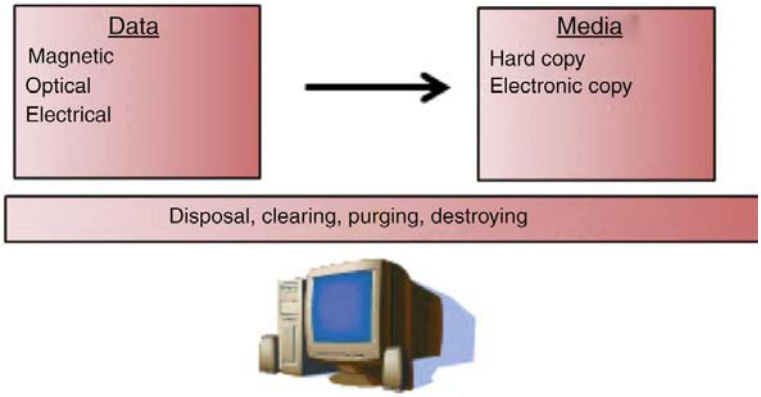
Information systems capture, process, and store information using a wide variety of media. This information is located not only on the intended storage media but also on devices used to create, process, or transmit this information. These media may require special disposition in order to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality. Efficient and effective management of information that is created, processed, and stored by an IT system throughout its life, from inception to disposition, is a primary concern of an information system owner and the custodian of the data.

With the use of increasingly sophisticated encryption, an attacker wishing to gain access to an organization's sensitive information is forced to look outside the system itself for that information. One avenue of attack is the recovery of supposedly deleted data from media. These residual data may allow unauthorized individuals to reconstruct data and thereby gain access to sensitive information. Sanitization can be used to thwart this attack by ensuring that deleted data cannot be easily recovered.

When storage media are transferred, become obsolete, or are no longer usable or required by an information system, it is important to ensure that residual magnetic, optical, electrical, or other representation of data that has been deleted is not easily recoverable. Sanitization

refers to the general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed.

Information disposition and sanitization decisions occur throughout the system life cycle. Critical factors affecting information disposition and media sanitization are decided at the start of a system's development. The initial system requirements should include hardware and software specifications as well as interconnections and data flow documents that will assist the system owner in identifying the types of media used in the system.



Types of Media

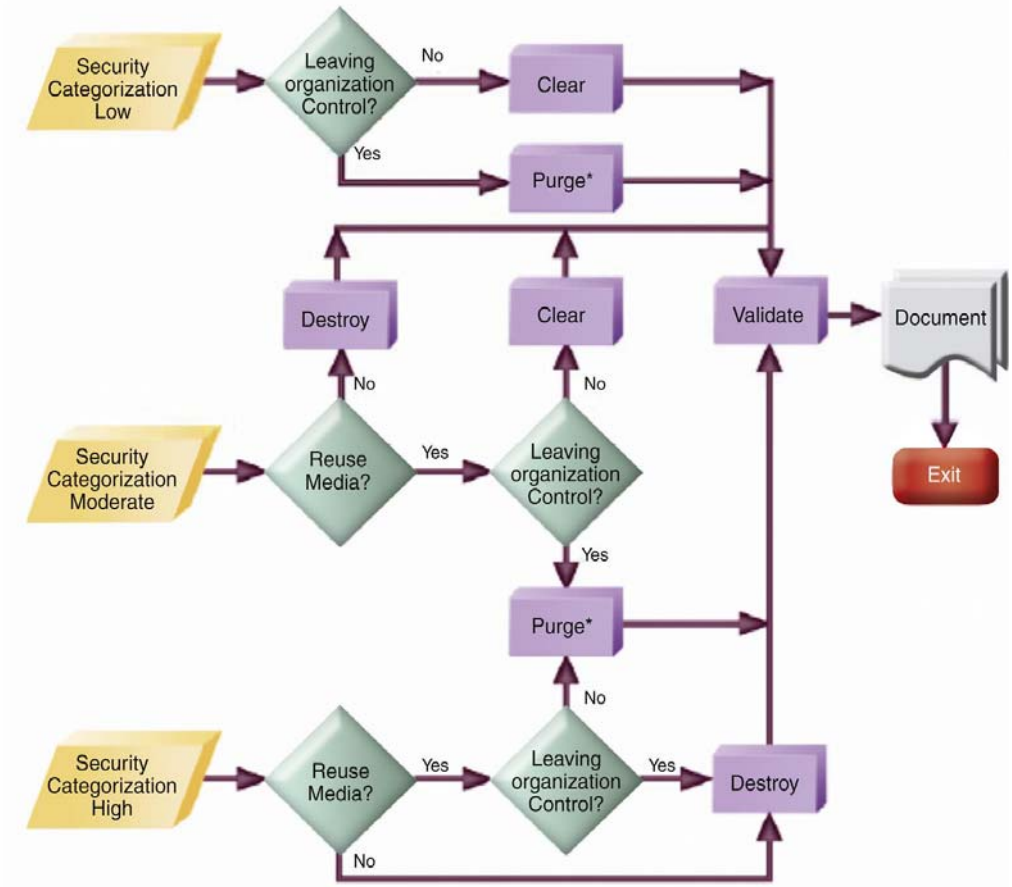
1. *Hard copy*: Hard copy media is physical representations of information. Paper printouts, printer, and facsimile ribbons, drums, and platens are all examples of hard copy media. These types of media are often the most uncontrolled. Information tossed into the recycle bins and trash containers exposes a significant vulnerability to "dumpster divers," and overcurious employees, risking accidental disclosures.
2. *Electronic (or soft copy)*: Electronic media are the bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment, and many other types.

There are different types of sanitization for each type of media. Media sanitization is divided into four categories in NIST SP 800-88: disposal, clearing, purging, and destroying.

1. *Disposal* is the act of discarding media with no other sanitization considerations. This is most often done by paper recycling containing nonconfidential information but may also include other media.
2. *Clearing* information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Simple deletion of items would not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities. It must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. For example, overwriting is an acceptable method for clearing media.
3. *Purging* information is a media sanitization process that protects the confidentiality of information against a laboratory attack. For some media, clearing media would not suffice for purging. However, for Advanced Technology Attachment (ATA) disk drives manufactured after 2001 (over 15 GB) the terms clearing and purging have converged.

4. *Destruction* of media is the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting.

Sanitization and Disposition Decision Flow



Organizations make sanitization decisions that are commensurate with the security categorization of the confidentiality of information contained on their media. The decision process is based on the confidentiality of the information, not the type of media. Once organizations decide what type of sanitization is best for their individual case, the media type will influence the technique used to achieve this sanitization goal.

Storage Encryption Technologies

SP 800-111 provides a high-level overview of the most commonly used options for encrypting stored information: full disk encryption (FDE), volume and virtual disk encryption, and file/folder encryption. It briefly defines each option and explains at a high level how it works.

1. *FDE*, also known as whole disk encryption, is the process of encrypting all the data on the hard drive used to boot a computer, including the computer's OS, and permitting access to the data only after successful authentication to the FDE product. Most FDE products are software-based.

   FDE software works by redirecting a computer's master boot record (MBR), which is a reserved sector on bootable media that determines which software (e.g., OS, utility) will be executed when the computer boots from the media. Before FDE software is installed onto a computer, the MBR usually points to the computer's primary OS. When FDE software is being used, the computer's MBR is redirected to a special preboot environment (PBE) that controls access to the computer.

   FDE software is most commonly used on desktop and laptop computers. The requirement for preboot authentication means that users have to be able to authenticate using the most fundamental components of a device, such as a standard keyboard – because the OS is not loaded, OS-level drivers are unavailable. For example, a personal digital assistant (PDA) or smart phone could not display a keyboard on the screen for entering a password because that is an OS-level capability.
2. *Virtual disk encryption* is the process of encrypting a file called a container, which can hold many files and folders, and permitting access to the data within the container only after proper authentication is provided, at which point the container is typically mounted as a virtual disk. Virtual disk encryption is used on all types of end user device storage. The container is a single file that resides within a logical volume. Examples of volumes are boot, system, and data volumes on a PC, and a Universal Serial Bus (USB) flash drive formatted with a single file system.

Characteristic	Full disk encryption	Volume encryption	Virtual disk encryption	File/folder encryption
Typical platforms supported	Desktop and laptop computers	Desktop and laptop computers, volume-based removable media (e.g., USB flash drives)	All types of end user devices	All types of end user devices
Data protected by encryption	All data on the media (data files, system files, residual data, and metadata)	All data in the volume (data files, system files, residual data, and metadata)	All data in the container (data files, residual data, and metadata, but not system files)	Individual files/folders (data files only)
Mitigates threats involving loss or theft of devices?	Yes	Yes	Yes	Yes
Mitigates OS and application layer threats (such as malware and insider threats)?	No	If the data volume is being protected, it sometimes mitigates such threats. If the data volume is not being protected, then there is no mitigation of these threats	It sometimes mitigates such threats	It sometimes mitigates such threats

(*Continued*)

Characteristic	Full disk encryption	Volume encryption	Virtual disk encryption	File/folder encryption
Potential impact to devices in case of solution failure	Loss of all data and device functionality	Loss of all data in volume; can cause loss of device functionality, depending on which volume is being protected	Loss of all data in container	Loss of all protected files/folders
Portability of encrypted information	Not portable	Not portable	Portable	Often portable

3. *Volume encryption* is the process of encrypting an entire logical volume and permitting access to the data on the volume only after proper authentication is provided. It is most often performed on hard drive data volumes and volume-based removable media, such as USB flash drives and external hard drives.

   The key difference between volume and virtual disk encryption is that containers are portable and volumes are not – a container can be copied from one medium to another, with encryption intact. This allows containers to be burned to CDs and DVDs and to be used on other media that are not volume-based. Virtual disk encryption also makes it trivial to back up sensitive data; the container is simply copied to the backup server or media. Another advantage of virtual disk encryption over volume encryption is that virtual disk encryption can be used in situations where volume-based removable media needs to have both protected and unprotected storage; the volume can be left unprotected and a container placed onto the volume for the sensitive information.
4. *File encryption* is the process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided. Folder encryption is very similar to file encryption, only it addresses individual folders instead of files. Some OSs offer built-in file and/or folder encryption capabilities and many third-party programs are also available. Although folder encryption and virtual disk encryption sound similar – both a folder and a container are intended to contain and protect multiple files – there is a difference. A container is a single opaque file, meaning that no one can see what files or folders are inside the container until the container is decrypted. File/folder encryption is transparent, meaning that anyone with access to the file system can view the names and possibly other metadata for the encrypted files and folders, including files and folders within encrypted folders, if they are not protected through OS AC features. File/folder encryption is used on all types of storage for end user devices.

PHYSICAL SECURITY

As an assessor, physical security reviews are usually conducted via "security walk-throughs" which are inspections of the facilities and their various components. These "walk-throughs" are just that, walking through the facility looking at the various equipment, configurations, electrical panels, HVAC systems, generators, fire suppression systems, and

physical access on doors and rooms. The primary areas for physical ACs to review and inspect include:

- Badges
- Memory cards
- Guards
- Keys
- True-floor-to-true-ceiling wall construction, especially in data centers and controlled access rooms
- Fences
- Locks

The primary areas to review during inspections for fire safety and suppression systems include:

- Building operation
- Building occupancy
- Fire detection equipment such as the various kinds of sensors
- Fire extinguishment, including fire extinguishers and delivery mechanisms for rooms

Reviewing the physical security of the facilities also includes the supporting utilities and their delivery. This includes:

- Air-conditioning system
- Electric power distribution
- Heating plants
- Water
- Sewage
- Alternative power and its delivery to the facility

Some of the more critical areas to focus on include looking at the positive flow for both air and water such that the flow is out of the room, rather than into the room, and the point of delivery of the utilities to the facility – is it secure from tampering or inadvertent accidents?

PERSONNEL SECURITY

The PS component is often overlooked and not reviewed in detail by assessors. This area has critical issues in today's world with insider threats, lack of reviews for new or transferring employees, as well as dealing with the US government's requirements for PIV credentials necessary for all users on government systems. Some of the documents and regulations which cover this area include:

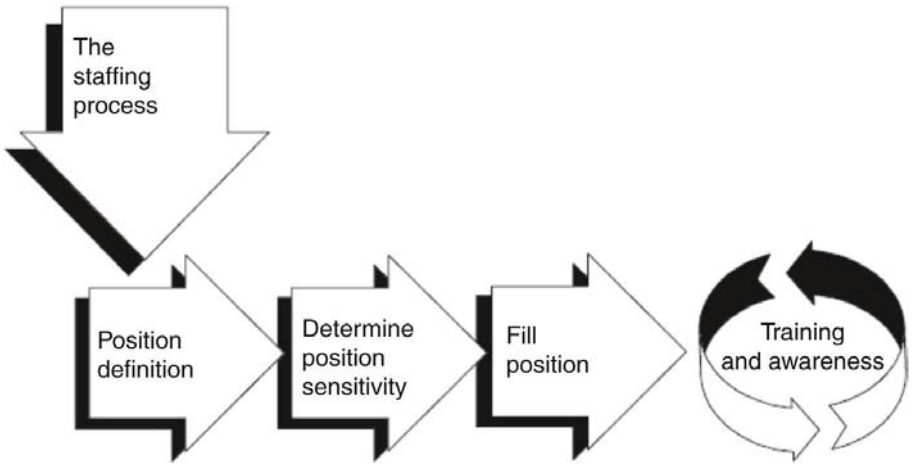
- 800-73
- 800-76
- 800-78
- 5 CFR 731.106, Designation of Public Trust Positions and Investigative Requirements
- ICD 704, Personnel Security Standards Sensitive Compartmented Information (SCI)

Proper information security practices should be in place to ensure that employees, contractors, and third-party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud, or misuse of facilities, specifically:

- Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment.
- All candidates for employment, contractors, and third-party users should be adequately screened, especially for sensitive jobs.
- Employees, contractors, and third-party users of information processing facilities should sign an agreement on their security roles and responsibilities.
- Security roles and responsibilities of employees, contractors, and third-party users should be defined and documented in accordance with the organization's information security policy.

The basic staffing process is shown below and the assessor should ensure the processes, procedures, and organizational policies provide the necessary guidance to the HR staff to accomplish these steps in a professional and secure manner throughout the recruitment, hiring, and employee life cycle for each and every employee and contractor involved in the governmental support efforts for their agency.

Staffing



Areas for coverage of personnel which the assessor should review include areas in user administration such as:

- User account management
- Audit and management reviews
- Detecting unauthorized/illegal activities
- Temporary assignments and in-house transfers
- Termination
  - Friendly termination
  - Unfriendly termination

Throughout the personnel process which is under review, the assessor should check on all of the user activities.

SYSTEM INTEGRITY

Integrity reviews often require an assessor to test a system capability either via automated tool employment or through the use of manual scripting efforts. These activities will require the assessor to have knowledge and skills in scripting languages and manual test development. Automated tool use will need the assessor to have experience in the use of the tool and the results expected from the tool. One of the principal ways of automated tool use is through employing vulnerability scanners which often can review the system and determine if there are configuration errors or misaligned areas of code within the application or the operating system. This includes patches for systems as well as code issues.

Patching and flaw remediation are areas of system integrity and system maintenance which the assessor should focus on first when testing and evaluating system integrity. Other areas are found in the following Special Publications:

- 800-40 – Patching (RA family of controls)
- 800-45 – Email
- 800-83 – Malware
- 800-92 – Logs (audit and accounting (AU) family of controls)

Malware Incident Prevention and Handling

SP 800-83, *Guide to Malware Incident Prevention and Handling*, provides recommendations for improving an organization's malware incident prevention measures. It also gives extensive recommendations for enhancing an organization's existing IR capability so that it is better prepared to handle malware incidents, particularly widespread ones. The recommendations address several major forms of malware, including viruses, worms, Trojan horses, malicious mobile code, blended attacks, spyware tracking cookies, and attacker tools such as backdoors and rootkits. The recommendations encompass various transmission mechanisms, including network services (e.g., email, web browsing, file sharing) and removable media.

The basic structure of SP 800-83 addresses focal points of interest for the assessor, such as:

- Malware categories
- Malware incident prevention:
  - Policy
  - Awareness
  - Vulnerability mitigation
  - Threat mitigation
- Malware IR

Malware Categories

- Viruses:
  - Compiled viruses

  - Interpreted viruses
  - Virus obfuscation techniques
- Worms
- Trojan horses
- Malicious mobile code
- Blended attacks
- Tracking cookies
- Attacker tools:
  - Backdoors
  - Keystroke loggers
  - Rootkits
  - Web browser plug-ins
  - Email generators
  - Attacker toolkits
- Non-malware threats:
  - Phishing
  - Virus hoaxes

This area of security should always be closely looked at and examined by the assessor as it is often used by attackers as one major area for exploitation of systems through many areas. Often I have found organizations only partially address flaws and remediation efforts and leave potential large and major exposures available for attacks to work against successfully.

Email Security – Spam

As the Special Publication, SP 800-45, states in the Executive Summary: "Electronic mail (email) is perhaps the most popularly used system for exchanging business information over the Internet (or any other computer network). At the most basic level, the email process can be divided into two principal components: (1) mail servers, which are hosts that deliver, forward, and store email; and (2) mail clients, which interface with users and allow users to read, compose, send, and store email. This document addresses the security issues of mail servers and mail clients, including Web-based access to mail.

Mail servers and user workstations running mail clients are frequently targeted by attackers. Because the computing and networking technologies that underlie email are ubiquitous and well-understood by many, attackers are able to develop attack methods to exploit security weaknesses. Mail servers are also targeted because they (and public Web servers) must communicate to some degree with untrusted third parties. Additionally, mail clients have been targeted as an effective means of inserting malware into machines and of propagating this code to other machines. As a result, mail servers, mail clients, and the network infrastructure that supports them must be protected."[21]

Understanding the email system within the organization requires understanding of the various potential attack and exposure areas such as:

[21]SP 800-45, p. ES-1.

- To exchange email with the outside world, a requirement for most organizations, it is allowed through organizations' network perimeter defenses. At a basic level, viruses and other types of malware may be distributed throughout an organization via email. Increasingly, however, attackers are getting more sophisticated and using email to deliver targeted zero-day attacks in an attempt to compromise users' workstations within the organization's internal network.
- Given email's nature of human to human communication, it can be used as a social engineering vehicle. Email can allow an attacker to exploit an organization's users to gather information or get the users to perform actions that further an attack.
- Flaws in the mail server application may be used as the means of compromising the underlying server and hence the attached network. Examples of this unauthorized access include gaining access to files or folders that were not meant to be publicly accessible, and being able to execute commands and/or install software on the mail server.
- Denial of service (DoS) attacks may be directed to the mail server or its support network infrastructure, denying or hindering valid users from using the mail server.
- Sensitive information on the mail server may be read by unauthorized individuals or changed in an unauthorized manner.
- Sensitive information transmitted unencrypted between mail server and client may be intercepted. All popular email communication standards default to sending usernames, passwords, and email messages unencrypted.
- Information within email messages may be altered at some point between the sender and recipient.
- Malicious entities may gain unauthorized access to resources elsewhere in the organization's network via a successful attack on the mail server. For example, once the mail server is compromised, an attacker could retrieve users' passwords, which may grant the attacker access to other hosts on the organization's network.
- Malicious entities may attack external organizations from a successful attack on a mail server host.
- Misconfiguration may allow malicious entities to use the organization's mail server to send email-based advertisements (i.e., spam).
- Users may send inappropriate, proprietary, or other sensitive information via email. This could expose the organization to legal action.[22]

The areas for the assessor to review should, therefore, include the following configuration items:

- Ensuring that spam cannot be sent from the mail servers they control
- Implementing spam filtering for inbound messages
- Blocking messages from known spam-sending servers

The assessor should examine the mail servers, clients, and organization's security architecture for the focal points as follows to ensure proper security for email systems:

1. Email message signing and encryption standards
2. Planning and management of mail servers
3. Securing the operating system underlying a mail server
4. Mail server application security
5. Email content filtering
6. Email-specific considerations in the deployment and configuration of network protection mechanisms, such as firewalls, routers, switches, and intrusion detection and intrusion prevention systems
7. Securing mail clients
8. Administering the mail server in a secure manner, including backups, security testing, and log reviews

[22]SP 800-45, p. ES1–ES2.

Each area should be tested for configuration, compliance, and actual security actions when dealing with this very sensitive organizational support area of email.

TECHNICAL AREAS OF CONSIDERATION

The common way for validating and verifying the technical controls is to employ automated testing tools and techniques as found in the NIST SP 800-115 testing guide. There are many tools which can be utilized to evaluate the various technical components, equipment, and configuration used by the IT staff, network support staff, and the agency. The basic four areas of technical controls are as follows:

1. AC
2. AU
3. IA
4. SC

We will examine each area and the parts of each with technical focus from an assessment perspective as we review the technical components that make up these controls.

ACCESS CONTROL

There are many NIST Special Publications for the various AC methodologies and implementations. Each one has a specific area of AC that it covers. Here are just some of the SPs available for review and reference as the controls are identified, implemented, and evaluated:

- 800-46 (Telework)
- 800-77 (Internet Protocol Security (IPSec))
- 800-113 (SSL)
- 800-114 (External Devices)
- 800-121 (Bluetooth)
- 800-48 (Legacy Wireless)
- 800-97 (802.11i Wireless)
- 800-124 (Cell Phones/PDA)
- OMB M 06-16 (Remote Access)

Logical Access Controls

Logical ACs are the primary means of managing and protecting resources to reduce risks to a level acceptable to an organization. They are tools used for identification, authentication, authorization, and accountability. They are software components that enforce AC measures for systems, programs, processes, and information. The logical ACs can be embedded within operating systems, applications, add-on security packages, or database and telecommunication management systems. In applying management-designed policies and procedures for protecting information assets, logical ACs are the primary means of managing and protecting

these resources to reduce risks to a level acceptable to an organization. For example, the concept of AC relates to managing and controlling access to an organization's information resources residing on host- and network-based computer systems. Assessors need to understand the relationship of logical ACs to management policies and procedures for information security. In doing so, assessors should be able to analyze and evaluate a logical AC's effectiveness in accomplishing information security objectives.

Inadequate logical ACs increase an organization's potential for losses resulting from exposures. These exposures can result in minor inconveniences up to a total shutdown of computer functions. Exposures that exist from accidental or intentional exploitation of logical AC weaknesses include technical exposures and computer crime.

For assessors to effectively assess logical ACs within the system under review, they first need to gain a technical and organizational understanding of the organization's IT environment. The purpose of this is to determine which areas from a risk standpoint warrant special attention in planning current and future work. This includes reviewing all security layers associated with the organization's IT information system architecture.

These layers are as follows:

- Network layer
- Operating system platform layer
- Database layer
- Application layer

Paths of Logical Access

Access or points of entry to an organization's information system infrastructure can be gained through several avenues. Each avenue is subject to appropriate levels of access security. For example, paths of logical access often relate to different levels occurring from either a back-end or a front-end interconnected network of systems for internally or externally based users. Front-end systems are network-based systems connecting an organization to outside untrusted networks, such as corporate websites, where a customer can access the website externally in initiating transactions that connect to a proxy server application which in turn connects, for example, to a back-end database system in updating a customer database. Front-end systems can also be internally based in automating business, paper-less processes that tie into back-end systems in a similar manner.

General Points of Entry

- General points of entry to either front-end or back-end systems relate to an organization's networking or telecommunications infrastructure in controlling access into their information resources (e.g., applications, databases, facilities, networks). The approach followed is based on a client–server model where, for example, a large organization can literally have thousands of interconnected network servers. Connectivity in this environment needs to be controlled through a smaller set of primary domain controlling servers, which enable a user to obtain access to specific secondary points of entry (e.g., application servers, databases).

General modes of access into this infrastructure occur through the following:

- Network connectivity
- Remote access
- Operator console
- Online workstations or terminals

Logical Access Control Software

IT has made it possible for computer systems to store and contain large quantities of sensitive data, increase the capability of sharing resources from one system to another, and permit many users to access the system through internet/intranet technologies. All of these factors have made organizations' information system resources more accessible and available anytime and anywhere.

To protect an organization's information resources, AC software has become even more critical in assuring the confidentiality, integrity, and availability of information resources. The purpose of AC software is *to prevent unauthorized access and modification to an organization's sensitive data and use of system critical functions*.

To achieve this level of control, it is necessary to apply ACs across all layers of an organization's information system architecture. This includes networks, platforms or operating system, databases, and application systems. Attributes across each commonly include some form of IA, access authorization, checking to specific information resources, and logging and reporting of user activities.

The greatest degree of protection in applying AC software is at the network and platform/operating system levels. These layers provide the greatest degree of protection of information resources from internal and external users' unauthorized access. These systems are also referred to as general support systems, and they make up the primary infrastructure on which applications and database systems will reside.

Operating system AC software interfaces with other system software AC programs, such as network layer devices (e.g., routers, firewalls), that manage and control external access to organizations' networks. Additionally, operating system AC software interfaces with database and/or application system ACs to protect system libraries and user datasets.

Logical Access Control Software Functionality

1. *General operating system AC functions include*:
   - **a.** Apply user IA mechanisms.
   - **b.** Restrict log-on IDs to specific terminals/workstations and specific times.
   - **c.** Establish rules for access to specific information resources (e.g., system-level application resources and data).
   - **d.** Create individual accountability and auditability.
   - **e.** Create or change user profiles.
   - **f.** Log events.
   - **g.** Log user activities.
   - **h.** Report capabilities.

2. *Database and/or application-level AC functions include*:
   a. Create or change data files and database profiles.
   b. Verify user authorization at the application and transaction levels.
   c. Verify user authorization within the application.
   d. Verify user authorization at the field level for changes within a database.
   e. Verify subsystem authorization for the user at the file level.
   f. Log database/data communications access activities for monitoring access violations.

Assessing ACs and AC systems:

- Start with obtaining a general understanding of the security risks facing information processing, through a review of relevant documentation, inquiry, observation, and risk assessment and evaluation techniques.
- Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency, and effectiveness by reviewing appropriate hardware and software security features and identifying any deficiencies or redundancies.
- Test controls over access paths to determine whether they are functioning and effective by applying appropriate testing techniques.
- Evaluate the AC environment to determine if the control requirements are achieved by analyzing test results and other evidence.
- Evaluate the security environment to assess its adequacy by reviewing written policies, and observing practices and procedures, and comparing them with appropriate security standards or practices and procedures used by other organizations.
- Familiarization with the IT environment:
  - This is the first step of the evaluation and involves obtaining a clear understanding of the technical, managerial, and security environment of the information system processing facility. This typically includes interviews, physical walk-throughs, review of documents, and risk assessments, as mentioned above in the physical security control area.
- Documenting the access paths:
  - The access path is the logical route an end user takes to access computerized information. This starts with a terminal/workstation and typically ends with the data being accessed. Along the way, numerous hardware and software components are encountered. The assessor should evaluate each component for proper implementation and proper physical and logical access security.
- Interviewing systems personnel:
  - To control and maintain the various components of the access path, as well as the operating system and computer mainframe, technical experts often are required. These people can be a valuable source of information to the assessor when gaining an understanding of security. To determine who these people are, the assessor should interview with the IS manager and review organizational charts and job descriptions. Key people include the security administrator, network control manager, and systems software manager.

- Reviewing reports from AC software:
  - The reporting features of AC software provide the security administrator with the opportunity to monitor adherence to security policies. By reviewing a sample of security reports, the assessor can determine if enough information is provided to support an investigation and if the security administrator is performing an effective review of the report.
- Reviewing Application Systems Operations Manual:
  - An Application Systems Manual should contain documentation on the programs that generally are used throughout a data processing installation to support the development, implementation, operations, and use of application systems. This manual should include information about which platform the application can run on, database management systems, compilers, interpreters, telecommunications monitors, and other applications that can run with the application.
- Log-on IDs and passwords:
  - To test confidentiality, the assessor could attempt to guess the password of a sample of employees' log-on IDs (though this is not necessarily a test). This should be done discreetly to avoid upsetting employees. The assessor should tour end user and programmer work areas looking for passwords taped to the side of terminals or the inside of desk drawers, or located in card files. Another source of confidential information is the wastebasket. The assessor might consider going through the office wastebasket looking for confidential information and passwords. Users could be asked to give their password to the assessor. However, unless specifically authorized for a particular situation and supported by the security policy, no user should ever disclose his/her password.
- Controls over production resources:
  - Computer ACs should extend beyond application data and transactions. There are numerous high-level utilities, macro or job control libraries, control libraries, and system software parameters for which AC should be particularly strong. Access to these libraries would provide the ability to bypass other ACs. The assessor should work with the system software analyst and operations manager to determine if access is on a need-to-know basis for all sensitive production resources. Working with the security administrator, the assessor should determine who can access these resources and what can be done with this access.
- Logging and reporting of computer access violations:
  - To test the reporting of access violations, the assessor should attempt to access computer transactions or data for which access is not authorized. The attempts should be unsuccessful and identified on security reports. This test should be coordinated with the data owner and security administrator to avoid violation of security regulations.
- Follow up access violations:
  - To test the effectiveness and timeliness of the security administrator's and data owner's response to reported violation attempts, the assessor should select a sample

of security reports and look for evidence of follow-up and investigation of access violations. If such evidence cannot be found, the assessor should conduct further interviews to determine why this situation exists.

- Identification of methods for bypassing security and compensating controls:
  - This is a technical area of review. As a result, the assessor should work with the system software analyst, network manager, operations manager, and security administrator to determine ways to bypass security. This typically includes bypass label processing (BLP), special system maintenance log-on IDs, operating system exits, installation utilities, and I/O devices. Working with the security administrator, the assessor should determine who can access these resources and what can be done with this access. The assessor should determine if access is on a need-to-know/have basis or if compensating detective controls exist.
- Review ACs and password administration:
  - Ensure password control is active for all accounts and users. Ensure password complexity and renewal requirements are enforced for all users and accounts. Ensure password criteria for elevated privilege accounts are more complex and longer than for standard user accounts as part of Separation of Duties review.
- Restricting and monitoring access:
  - There should be restrictions and procedures of monitoring access to computer features that bypass security. Generally, only system software programmers should have access to these features:
    - *BLP*: BLP bypasses the computer reading of the file label. Since most AC rules are based on file names (labels), this can bypass access security.
    - *System exits*: This system software feature permits the user to perform complex system maintenance, which may be tailored to a specific environment or company. They often exist outside of the computer security system and, thus, are not restricted or reported in their use.
    - *Special system log-on IDs*: These log-on IDs often are provided with the computer by the vendor. The names can be determined easily because they are the same for all similar computer systems. Passwords should be changed immediately, on installation, to secure the systems.
- Auditing remote access:
  - Remote use of information resources dramatically improves business productivity, but generates control issues and security concerns. In this regard, IS auditors should determine that all remote access capabilities used by an organization provide for effective security of the organization's information resources. Remote access security controls should be documented and implemented for authorized users operating outside of the trusted network environment. In reviewing existing remote access architectures, IS auditors should assess remote access points (APs) of entry in addressing how many (known/unknown) exist and whether greater centralized control of remote APs is needed. IS auditors should also review APs for appropriate

controls, such as in the use of virtual private networks (VPNs), authentication mechanisms, encryption, firewalls, and IDS.

IDENTIFICATION AND AUTHENTICATION

IA is the process of proving one's identity. It is the process by which the system obtains from a user his/her claimed identity and the credentials needed to authenticate this identity, and validates both pieces of information.

LOG-ON IDS AND PASSWORDS

Features of passwords:

- A password should be easy for the user to remember but difficult for a perpetrator to guess.
- Initial passwords may be allocated by the security administrator or generated by the system itself. When the user logs on for the first time, the system should force a password change to improve confidentiality.
- If the wrong password is entered a predefined number of times, typically three, the log-on ID should be automatically and permanently deactivated (or at least for a significant period of time).

Token Devices, One-Time Passwords

A two-factor authentication technique, such as a microprocessor-controlled smart card, generates one-time passwords that are good for only one log-on session. Users enter this password along with a password they have memorized to gain access to the system. This technique involves something you have (a device subject to theft) and something you know (a personal identification number). Such devices gain their one-time password status because of a unique session characteristic (e.g., ID or time) appended to the password.

Biometrics

Biometric ACs are the best means of authenticating a user's identity based on a unique, measurable attribute or trait for verifying the identity of a human being. This control restricts computer access, based on a physical (something you are) or behavioral (something you do) characteristic of the user.

Management of Biometrics

Management of biometrics should address effective security for the collection, distribution, and processing of biometric data.

Management should develop and approve biometric information management and security (BIMS) policy. The auditor should use the BIMS policy to gain a better understanding of the biometric systems in use.

Single Sign-On (SSO)

Users normally require access to a number of resources during the course of their daily routine. For example, users would first log into an operating system and thereafter into various applications. For each operating system application or other resource in use, the user is required to provide a separate set of credentials to gain access; this results in a situation wherein the user's ability to remember passwords is significantly reduced. This situation also increases the chance that a user will write them down on or near their workstation or area of work, and thereby increase the risks that a security breach within the organization may occur.

To address this situation, the concept of SSO was developed. SSO can generally be defined as the process for consolidating all organization platform-based administration, authentication, and authorization functions into a single centralized administrative function. This function would provide the appropriate interfaces to the organization's information resources, which may include:

- Client–server and distributed systems
- Mainframe systems
- Network security including remote access mechanisms

The SSO process begins with the first instance where the user credentials are introduced into the organization's IT computing environment. The information resource or SSO server handling this function is referred to as the primary domain. Every other information resource, application, or platform that uses those credentials is called a secondary domain.

The authorization process of AC often requires that the system be able to identify and differentiate among users. For example, AC is often based on least privilege, which refers to the granting to users of only those accesses required to perform their duties.

Access rules (authorization) specify who can access what. Access should be on a documented need-to-know and need-to-do basis by type of access.

Having computer access does not always mean unrestricted access. Computer access can be set to many differing levels. When IS auditors review computer accessibility, they need to know what can be done with the access and what is restricted. For example, access restrictions at the file level generally include the following:

- Read, inquiry, or copy only
- Write, create, update, or delete only
- Execute only
- A combination of the above

Authentication of an individual's identity is a fundamental component of physical and logical AC processes. When an individual attempts to access security-sensitive buildings, computer systems, or data, an AC decision must be made. An accurate determination of identity is needed to make sound AC decisions.

A wide range of mechanisms is employed to authenticate identity, utilizing various classes of identity credentials. For physical access, individual identity has traditionally been authenticated by use of paper or other nonautomated, hand-carried credentials, such as driver's licenses and badges. Access authorization to computers and data has traditionally been authenticated through user-selected passwords. More recently, cryptographic mechanisms and

biometric techniques have been used in physical and logical security applications, replacing or supplementing the traditional credentials.

The strength of the authentication that is achieved varies, depending on the type of credential, the process used to issue the credential, and the authentication mechanism used to validate the credential. This document establishes a standard for a PIV system based on secure and reliable forms of identification credentials issued by the federal government to its employees and contractors. These credentials are intended to authenticate individuals who require access to federally controlled facilities, information systems, and applications.

SYSTEMS AND COMMUNICATIONS PROTECTION

Network Layer Security

There are multiple methods and techniques employed by organizations for deploying and enhancing network security. All methods provide differing levels of confidentiality, integrity, and availability depending on their technology, location on the network, and method of installation. We will highlight several of these methods to properly review, examine, and evaluate each to ensure the use of and actions conducted by these methods are functional, operational, and secure. We will start with VPNs, and then discuss wireless networking, IDS, encryption, and firewalls.

VPN

A VPN is a virtual network, built on top of existing physical networks, which can provide a secure communications mechanism for data and other information transmitted between networks. Because a VPN can be used over existing networks, such as the internet, it can facilitate the secure transfer of sensitive data across public networks. This is often less expensive than alternatives such as dedicated private telecommunications lines between organizations or branch offices. We will examine the two most common types of VPNs utilized in today's networks in order to properly assess them: IPSec and SSL-based VPNs. "IPsec has emerged as the most commonly used network layer security control for protecting communications, while SSL is the most commonly used transport layer security control. Depending on how IPsec and SSL are implemented and configured, both can provide any combination of the following types of protection:

- **Confidentiality.** IPsec and SSL can ensure that data cannot be read by unauthorized parties. This is accomplished by encrypting data using a cryptographic algorithm and a secret key—a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key.
- **Integrity.** IPsec and SSL can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a keyed cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.

- **Peer Authentication.** Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host. SSL authentication is typically performed one-way, authenticating the server to the client; however, SSL VPNs require authentication for both endpoints.
- **Replay Protection.** The same data is not delivered multiple times, and data is not delivered grossly out of order.
- **Traffic Analysis Protection.** A person monitoring network traffic cannot determine the contents of the network traffic or how much data is being exchanged. IPsec can also conceal which parties are communicating, whereas SSL leaves this information exposed. Frequency of communication may also be protected depending on implementation. Nevertheless, the number of packets being exchanged can be counted.
- **Access Control.** IPsec and SSL endpoints can perform filtering to ensure that only authorized users can access particular network resources. IPsec and SSL endpoints can also allow or block certain types of network traffic, such as allowing Web server access but denying file sharing."[23]

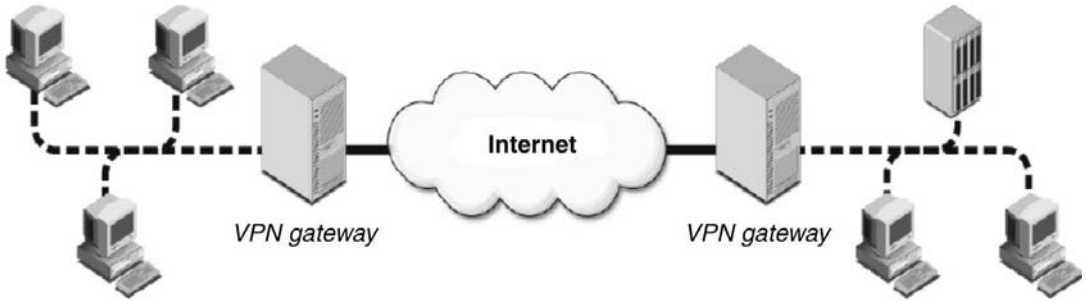
So we start with IPSec VPNs, and then we will discuss SSL/Transport Layer Security (TLS) VPNs.

IPSec VPN – SP 800-77

IPSec is a framework of open standards for ensuring private communications over public networks. It has become one of the most common network layer security controls, typically used to create a VPN.

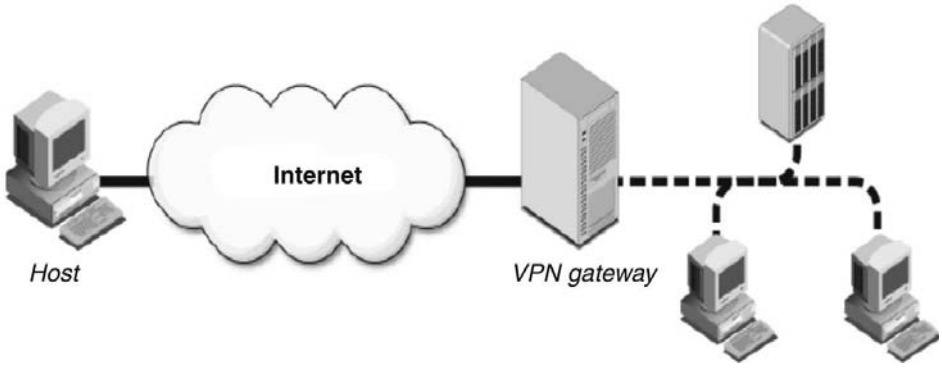
There are three primary models for VPN architectures, as follows:

1. *Gateway-to-gateway*: This model protects communications between two specific networks, such as an organization's main office network and a branch office network, or two business partners' networks.

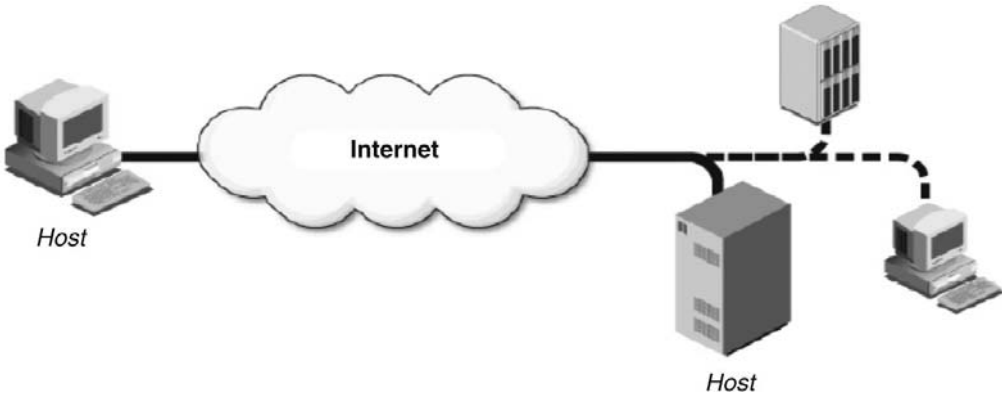


2. *Host-to-gateway*: This model protects communications between one or more individual hosts and a specific network belonging to an organization. The host-to-gateway model is most often used to allow hosts on unsecured networks, such as traveling employees and telecommuters, to gain access to internal organizational services, such as the organization's email and web servers.

[23]SP 800-113, p. 2-3, 2-4.



3. *Host-to-host*: A host-to-host architecture protects communication between two specific computers. It is most often used when a small number of users need to use or administer a remote system that requires the use of inherently insecure protocols.



VPN Model Comparison

Feature	Gateway-to-gateway	Host-to-gateway	Host-to-host
Provides protection between client and local gateway	No	N/A (client is VPN end point)	N/A (client is VPN end point)
Provides protection between VPN end points	Yes	Yes	Yes
Provides protection between remote gateway and remote server (behind gateway)	No	No	N/A (server is VPN end point)
Transparent to users	Yes	No	No
Transparent to users' systems	Yes	No	No
Transparent to servers	Yes	Yes	No

IPSec is a collection of protocols that assist in protecting communications over IP networks. IPSec protocols work together in various combinations to provide protection for communications.

- IPsec fundamentals:
  - *Authentication Header (AH)*: AH, one of the IPSec security protocols, provides integrity protection for packet headers and data, as well as user authentication. It can optionally provide replay protection and access protection. AH cannot encrypt any portion of packets.
  - *AH modes*: AH has two modes – *transport* and *tunnel*. In tunnel mode, AH creates a new IP header for each packet; in transport mode, AH does not create a new IP header. In IPSec architectures that use a gateway, the true source or destination IP address for packets must be altered to be the gateway's IP address. Because transport mode cannot alter the original IP header or create a new IP header, transport mode is generally used in host-to-host architectures.
  - *Encapsulating Security Payload (ESP)*: ESP is the second core IPSec security protocol. In the initial version of IPSec, ESP provided only encryption for packet payload data. Integrity protection was provided by the AH protocol if needed. In the second version of IPSec, ESP became more flexible. It can perform authentication to provide integrity protection, although not for the outermost IP header. Also, ESP's encryption can be disabled through the Null ESP Encryption Algorithm. Therefore, in all but the oldest IPSec implementations, ESP can be used to provide only encryption, encryption and integrity protection, or only integrity protection.

    ESP has two modes: *transport* and *tunnel*. In tunnel mode, ESP creates a new IP header for each packet. The new IP header lists the end points of the ESP tunnel (such as two IPSec gateways) as the source and destination of the packet. Because of this, tunnel mode can be used with all three VPN architecture models.
  - *Internet Key Exchange (IKE)*: The purpose of the IKE protocol is to negotiate, create, and manage security associations (SAs). *SA* is a generic term for a set of values that define the IPSec features and protections applied to a connection. SAs can also be manually created, using values agreed upon in advance by both parties, but these SAs cannot be updated; this method does not scale for real-life large-scale VPNs. IKE uses five different types of exchanges to create SAs, transfer status and error information, and define new Diffie–Hellman groups. In IPSec, IKE is used to provide a secure mechanism for establishing IPsec-protected connections.
  - *IP Payload Compression Protocol (IPComp)*: In communications, it is often desirable to perform lossless compression on data – to repackage information in a smaller format without losing any of its meaning. The IPComp is often used with IPSec. By applying IPComp to a payload first, and then encrypting the packet through ESP, effective compression can be achieved.

    IPComp can be configured to provide compression for IPSec traffic going in one direction only (e.g., compress packets from end point A to end point B, but not from end point B to end point A) or in both directions. Also, IPComp allows administrators to choose from multiple compression algorithms, including DEFLATE and LZS.49. IPComp provides a simple yet flexible solution for compressing IPSec payloads.

IPComp can provide lossless compression for IPSec payloads. Because applying compression algorithms to certain types of payloads may actually make them larger, IPComp compresses the payload only if it will actually make the packet smaller. IPSec uses IKE to create SAs, which are sets of values that define the security of IPsec-protected connections. IKE phase 1 creates an IKE SA; IKE phase 2 creates an IPSec SA through a channel protected by the IKE SA. IKE phase 1 has two modes: main mode and aggressive mode. Main mode negotiates the establishment of the bidirectional IKE SA through three pairs of messages, while aggressive mode uses only three messages. Although aggressive mode is faster, it is also less flexible and secure. IKE phase 2 has one mode: quick mode. Quick mode uses three messages to establish a pair of unidirectional IPSec SAs. Quick mode communications are encrypted by the method specified in the IKE SA created by phase 1.

SSL VPNs – SP 800-113

An SSL VPN consists of one or more VPN devices to which users connect using their web browsers. The traffic between the web browser and the SSL VPN device is encrypted with the SSL protocol or its successor, the TLS protocol. This type of VPN may be referred to as either an SSL VPN or a TLS VPN.

> Secure Sockets Layer (SSL) virtual private networks (VPN) provide secure remote access to an organization's resources. An SSL VPN consists of one or more VPN devices to which users connect using their Web browsers. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol or its successor, the Transport Layer Security (TLS) protocol. This type of VPN may be referred to as either an SSL VPN or a TLS VPN. This guide uses the term SSL VPN. SSL VPNs provide remote users with access to Web applications and client/server applications, and connectivity to internal networks. Despite the popularity of SSL VPNs, they are not intended to replace Internet Protocol Security (IPsec) VPNs.1 The two VPN technologies are complementary and address separate network architectures and business needs. SSL VPNs offer versatility and ease of use because they use the SSL protocol, which is included with all standard Web browsers, so the client usually does not require configuration by the user. SSL VPNs offer granular control for a range of users on a variety of computers, accessing resources from many locations.[24]

SSL PORTAL VPNS

An SSL portal VPN allows a user to use a single standard SSL connection to a website to securely access multiple network services. The site accessed is typically called a portal because it has a single page that leads to many other resources. SSL portal VPNs act as transport-layer VPNs that work over a single network port, namely the TCP port for SSL-protected HTTP (443).

SSL TUNNEL VPNS

An SSL tunnel VPN allows a user to use a typical web browser to securely access multiple network services through a tunnel that is running under SSL. SSL tunnel VPNs require that the web browser be able to handle specific types of active content (e.g., Java, JavaScript, Flash, or ActiveX) and that the user be able to run them. (Most browsers that handle such applications and plug-ins also allow the user or administrator to block them from being executed.)

[24]SP 800-113, p. ES-1.

ADMINISTERING SSL VPN

The administration of both SSL portal VPNs and SSL tunnel VPNs is similar. The gateway administrator needs to specify local policy in at least two broad areas:

- **Access**. All SSL VPNs allow the administrator to specify which users have access to the VPN services. User authentication might be done with a simple password through a Web form, or through more sophisticated authentication mechanisms.
- **Capabilities**. The administrator can specify the services to which each authorized user has access. For example, some users might have access to only certain Web pages, while others might have access to those Web pages plus other services.

Different SSL VPNs have very different administrative interfaces and very different capabilities for allowing access and specifying allowed actions for users. For example, many but not all SSL VPNs allow validation of users through the Remote Authentication Dial-In User Server (RADIUS) protocol. As another example, some SSL VPNs allow the administrator to create groups of users who have the same access methods and capabilities; this makes adding new users to the system easier than gateways that require the administrator to specify both of these for each new user.[25]

SSL VPN ARCHITECTURE

The five phases of the recommended approach are as follows:

1. **Identify Requirements.** Identify the requirements for remote access and determine how they can best be met.
2. **Design the Solution.** Make design decisions in five areas: access control, endpoint security, authentication methods, architecture, and cryptography policy.
3. **Implement and Test a Prototype.** Test a prototype of the designed solution in a laboratory, test, or production environment to identify any potential issues.
4. **Deploy the Solution.** Gradually deploy the SSL VPN solution throughout the enterprise, beginning with a pilot program.
5. **Manage the Solution.** Maintain the SSL VPN components and resolve operational issues. Repeat the planning and implementation process when significant changes need to be incorporated into the solution.[26]

Note: Many of the cryptographic algorithms used in some SSL cipher suites are not FIPS-approved, and therefore are not allowed for use in SSL VPNs that are to be used in applications that must conform to FIPS-140-2.

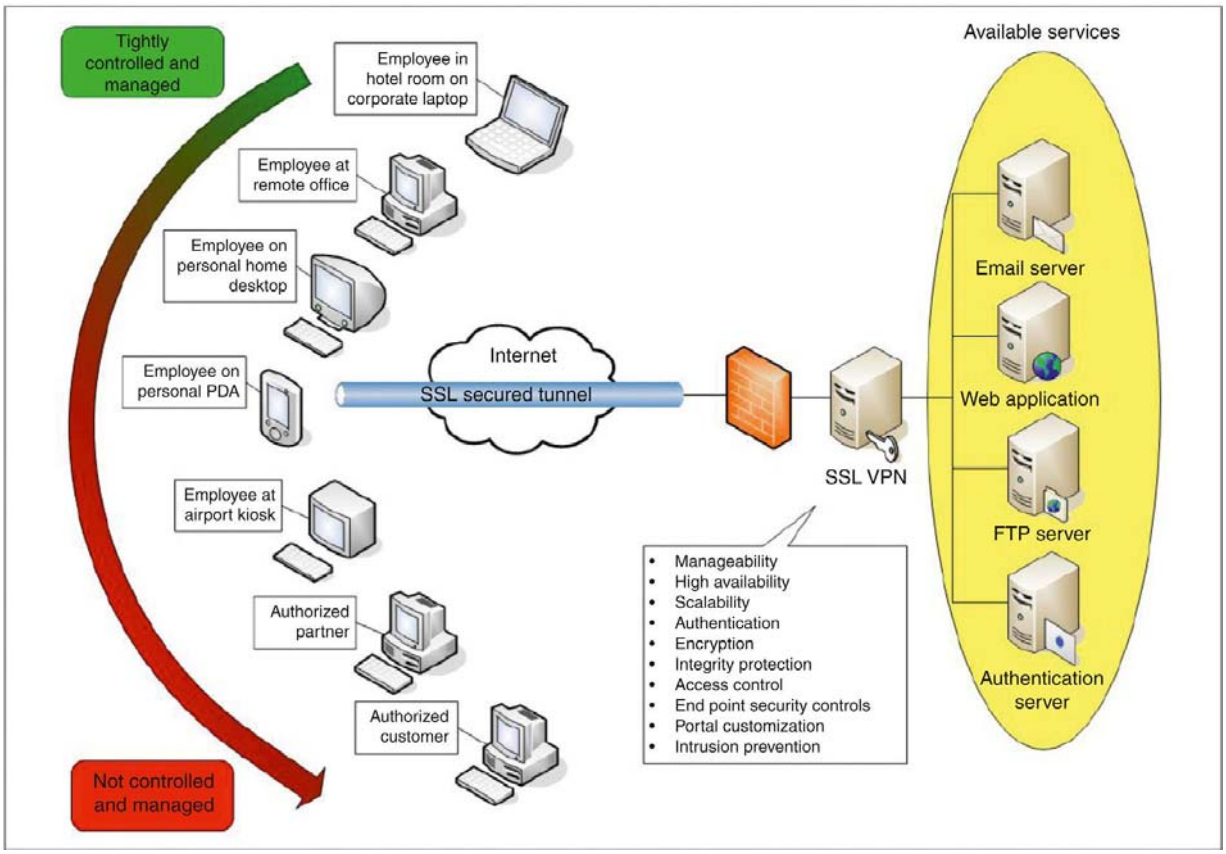
SSL VPN ARCHITECTURE

Typical SSL VPN users include people in remote offices, mobile users, business partners, and customers. Hardware clients include various types of devices, such as public kiosks, home personal computers (PC), PDAs, or smart phones, which may or may not be controlled or managed by the organization. The SSL VPN may also be accessed from any location including an airport, a coffee shop, or a hotel room, as long as the location has connectivity to the Internet and the user has a Web client that is capable of using the particular SSL VPN. All traffic is encrypted as it traverses public networks such as the Internet. The SSL VPN gateway is

[25]SP 800-113, p. 2-5, 2-6.

[26]SP 800-113, p. ES-3.

the end point for the secure connection and provides various services and features (most SSL VPN products are standalone hardware appliances, although there are some software-based solutions that are installed on user-supplied servers).[27]



SSL PROTOCOL BASICS

The security of the data sent over an SSL VPN relies on the security of the SSL protocol. The SSL protocol allows a client (such as a web browser) and a server (such as an SSL VPN) to negotiate the type of security to be used during an SSL session. Thus, it is critical to make sure that the security agreed to by the remote user and the SSL gateway meets the security requirements of the organization using the SSL VPN.

There are three types of security that the client and the server can negotiate: the version of SSL, the type of cryptography, and the authentication method.

- *Versions of SSL and TLS*: The terms SSL and TLS are often used together to describe the same protocol. In fact, SSL refers to all versions of the SSL protocol as defined by the Internet Engineering Task Force (IETF), while TLS refers only to versions 3.1 and later of the SSL protocol. Two versions of TLS have been standardized: TLS 1.0 and TLS 1.1.

[27] *Ibid.*, p. 3-1.

TLS 1.0 is the same as SSL 3.1; there are no versions of SSL after 3.1. As of the writing of this guide, work is being done on TLS version 1.2.

TLS is approved for use in the protection of federal information; SSL versions other than 3.1 are not.

- *Cryptography used in SSL sessions*: There are many types of cryptographic functions that are used in security protocols. The most widely known cryptographic features are confidentiality (secrecy of data), integrity (the ability to detect even minute changes in the data), and signature (the ability to trace the origin of the data). The combination of these features is an important aspect of the overall security of a communications stream. SSL uses four significant types of features: confidentiality, integrity, signature, and key establishment (the way that a key is agreed to by the two parties).

  SSL uses cipher suites to define the set of cryptographic functions that a client and a server use when communicating. This is unlike protocols such as IPSec and Secure/Multipurpose Internet Mail Extensions (S/MIME) where the two parties agree to individual cryptographic functions. That is, SSL exchanges say in effect, "Here is a set of functions to be used together, and here is another set I am willing to use." IPSec and S/MIME (and many other protocols) instead say, "Here are the confidentiality functions I am willing to use, here are the integrity functions I am willing to use, and here are the signature algorithms I am willing to use," and the other side creates a set from those choices.

  Just as the SSL client and server need to be able to use the same version of SSL, they also need to be able to use the same cipher suite; otherwise, the two sides cannot communicate. The organization running the SSL VPN chooses which cipher suites meet its security goals and configures the SSL VPN gateway to use only those cipher suites.
- *Authentication used for identifying SSL servers*: When a web browser connects to an SSL server such as an SSL VPN gateway, the browser user needs some way to know that the browser is talking to a server the user trusts. SSL uses certificates that are signed by trusted entities to authenticate the server to the web user. (SSL can also use certificates to authenticate users to servers, but this is rarely done.)

  The server authentication occurs very early in the SSL process, immediately after the user sends its first message to the SSL server. In that first message, the web browser specifies which type of certificate algorithms it can handle; the two common choices are RSA and DSS. In the second message, the SSL server responds with a certificate of one of the types that the browser said it understands. After receiving the certificate, the web browser verifies that the identity in the certificate (i.e., the domain name listed in the certificate) matches the domain name to which the web browser attempted to connect.

  Some SSL VPNs use certificates issued by the vendor of the SSL VPN, and those certificates do not link through a chain of trust to a root certificate that is normally trusted by most users. If that is the case, the user should add the SSL VPN's own certificate to the user's list of directly trusted certificates. It is important to note that users should not add the root certificate of the SSL VPN's manufacturer to the list of certification authorities that the user trusts, since the manufacturer's security policies and controls may differ from those of the organization. Other SSL VPNs produce self-signed certificates that do not chain to any trusted root certificate; as before, the user should add the SSL VPN's own certificate to the user's list of directly trusted certificates.

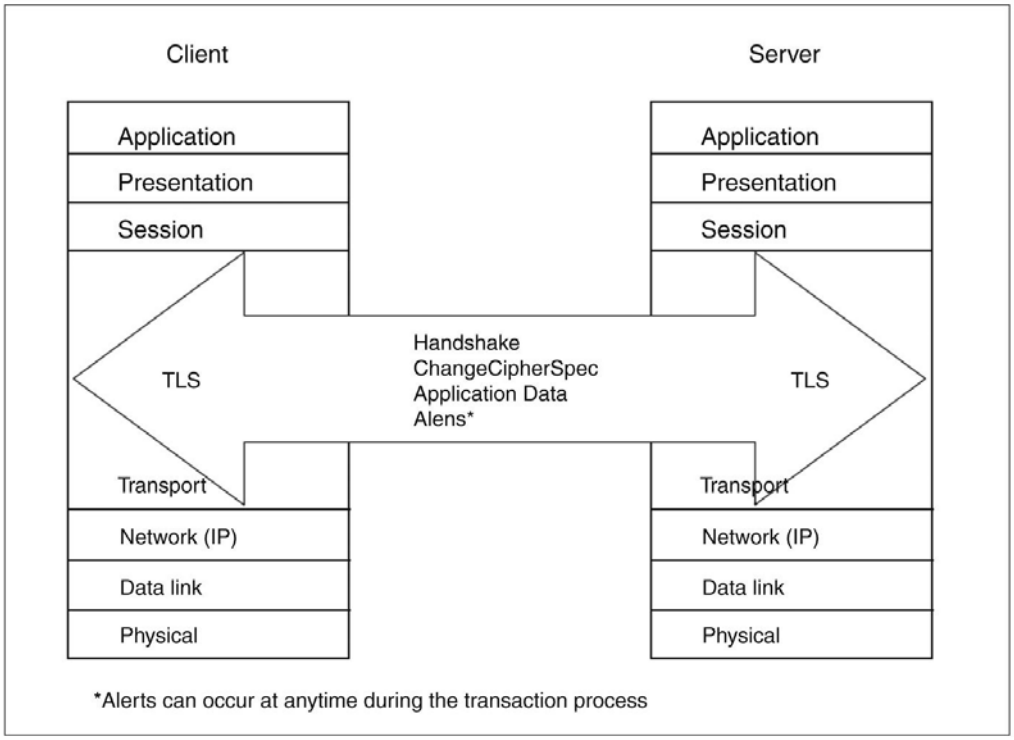
Transport Layer Security

The Netscape Corporation designed a protocol known as the SSL to meet security needs of client browsers and server applications. Version 1 of SSL was never released. Version 2 (SSL 2.0) was released in 1994 but had well-known security vulnerabilities. Version 3 (SSL 3.0) was released in 1995 to address these vulnerabilities.

During this timeframe, Microsoft Corporation released a protocol known as Private Communications Technology (PCT), and later released a higher performance protocol known as the Secure Transport Layer Protocol (STLP). PCT and STLP never commanded the market share that SSL 2.0 and SSL 3.0 commanded. The IETF (a technical working group responsible for developing internet standards to ensure communications compatibility across different implementations) attempted to resolve, as best it could, security engineering and protocol incompatibility issues between the protocols. The IETF standards track Transport Layer Security Protocol Version 1.0 (TLS 1.0) emerged and was codified by the IETF as [RFC2246].

While TLS 1.0 is based on SSL 3.0, and the differences between them are not dramatic, they are significant enough that TLS 1.0 and SSL 3.0 do not interoperate. However, TLS 1.0 does incorporate a mechanism by which a TLS 1.0 implementation can negotiate to use SSL 3.0 with requesting entities as if TLS were never proposed. However, because SSL 3.0 is not approved for use in the protection of federal information (Section 7.1 of [FIPS140-2l]), TLS must be properly configured to ensure that the negotiation and use of SSL 3.0 never occurs when federal information is to be protected.

The NIST guidelines (SP 800-52, SP 800-77, and SP 800-113) attempt to make clear the impact of selecting and using secure web transport protocols for use in protecting sensitive but unclassified US government information.



Both the TLS 1.0 and the SSL 3.0 protocol specifications use cryptographic mechanisms to implement the security services that establish and maintain a secure TCP/IP connection. The secure connection prevents eavesdropping, tampering, or message forgery. Implementing data confidentiality with cryptography (encryption) prevents eavesdropping, generating a message authentication code (MAC) with a secure hash function prevents undetected tampering, and authenticating clients and servers with public key cryptography-based digital signatures prevents message forgery. In each case – preventing eavesdropping, tampering, and forgery – a key or shared secret is required by the cryptographic mechanism. A pseudo-random number generator and a key establishment algorithm provide for the generation and sharing of these secrets.

The rows in the following table identify the key establishment, confidentiality, digital signature, and hash mechanisms currently in use today in TLS 1.0 and SSL 3.0. The columns identify which key establishment, confidentiality, and signature algorithms and which hash functions are FIPS.

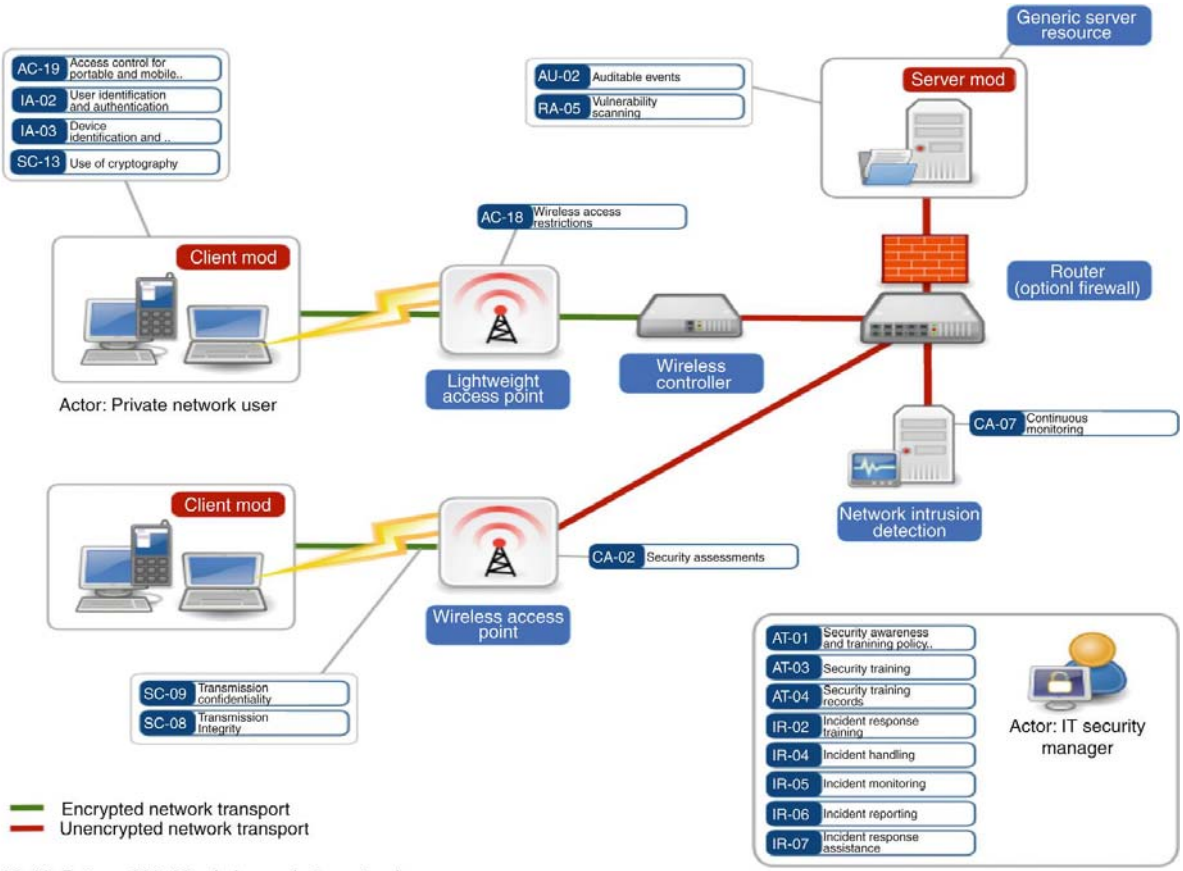
Mechanism	SSL (3.0)	TLS 1.0	FIPS reference
Key establishment	RSA	RSA	
	DH-RSA	DH-RSA	
	DH-DSS	DH-DSS	
	DHE-RSA	DHE-RSA	
	DHE-DSS	DHE-DSS	
	DH-Anon	DH-Anon	
	Fortezza-KEA		
Confidentiality	IDEA-CBC	IDEA-CBC	FIPS46-3.FIPS81
	RC4-128	RC4-128	
	3DES-EDE-CBC	3DES-EDE-CBC	
	Fortezza-CBC		
		Kerberos	
		AES	FIPS-197
Signature	RSA	RSA	FIPS-186-2
	DSA	DSA	FIPS-186-2
		EC	FIPS-186-2
Hash	MD5	MD5	
	SHA-1	SHA-1	FIPS-180-2, FIPS-198

WIRELESS NETWORKING

In today's networks, there are often many methods for communications used and deployed. Some of these methods take advantage of nonwired connectivity by utilizing wireless technology. There are several types of wireless-based networking methods currently used all based on radio-frequency (RF) methods of communications for the transmission and reception of the signals carrying the digital data across and external to the network. Examples of wireless networks include cell phone networks, Wi-Fi local networks, and terrestrial microwave networks.

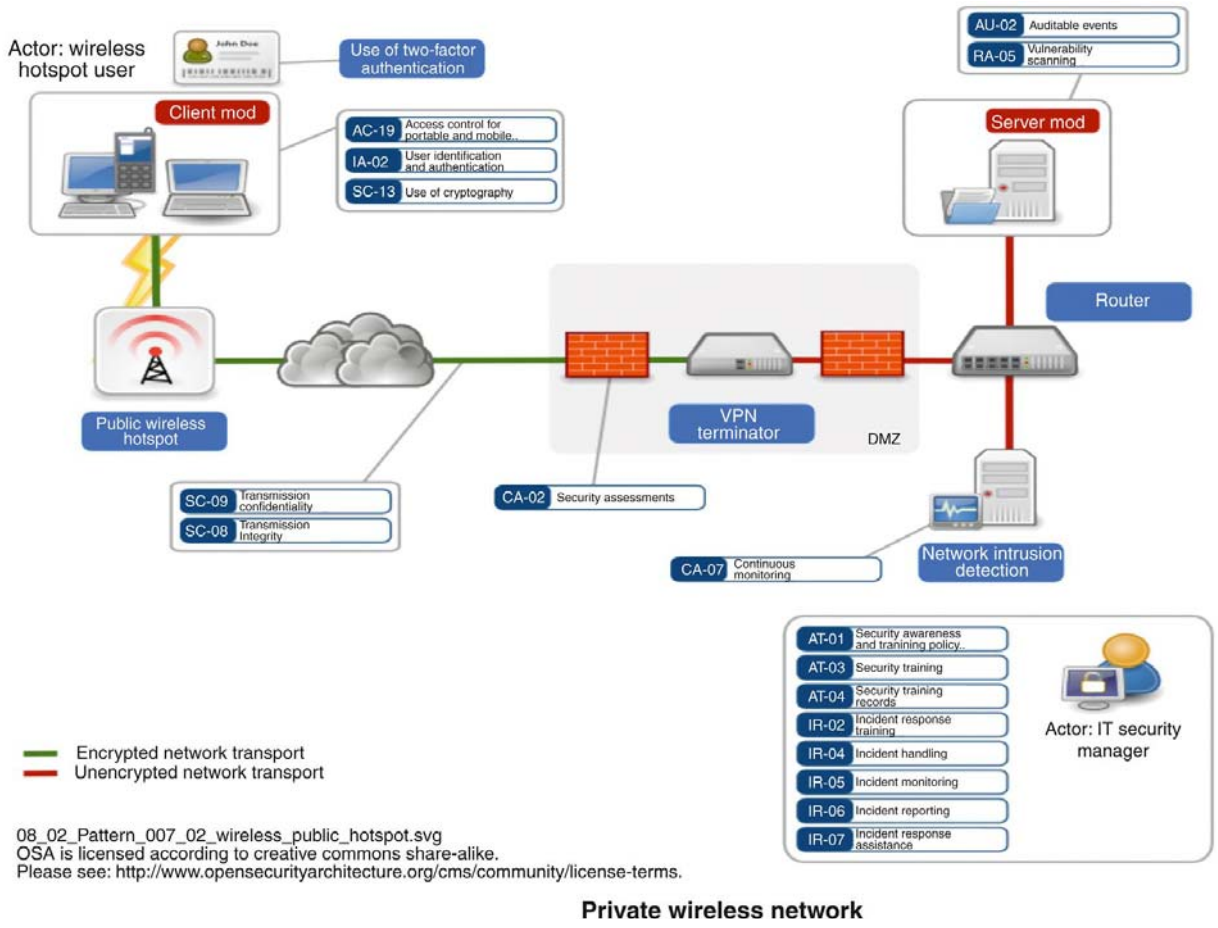
Every wireless LAN network consists of an AP, such as a wireless router, and one or more wireless adapters. As shown in the standard two deployment modes below, there are many security controls from SP 800-53 which are applicable and necessary to secure wireless LANs and Wi-Fi networks. The assessor needs to focus on the technology deployed, review all design and implementation documents, and test the actual APs (aka hotspots) and the client adapters used to prove the encryption and communications used during the wireless activities remain active and constant during all phases of transmission of the data over the airwaves via the RF signals used.

A *wireless AP* is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. The AP usually connects to a router (via a wired network) as a stand-alone device, but it can also be an integral component of the router itself. An AP is differentiated from a hotspot, which is the physical space where the wireless service is provided. A hotspot is a common public application of APs, where wireless clients can connect to the internet without regard for the particular networks to which they have attached for the moment.



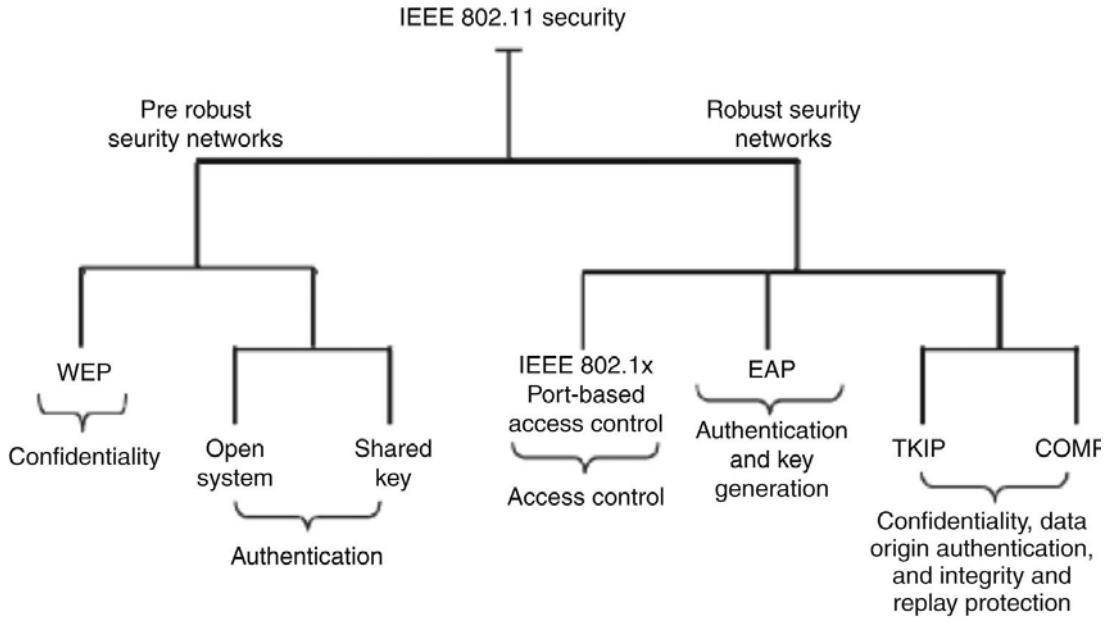
08_02_Pattern_006_02_wireless_private_network.svg
OSA is licensed according to creative commons share-alike.
Please see: http://www.opensecurityarchitecture.org/cms/community/license-terms.

Private wireless network



Private wireless network

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks by utilizing different methods of encoding and encryption, based on the parameters of the RF carrier and bandwidth used by the particular type of Wi-Fi being employed. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999 which was outdated in 2003 by WPA or WPA. WPA was a quick alternative to improve security over WEP. The current standard is WPA2 which uses an encryption mechanism which encrypts the network with a 256-bit key; the longer key length improves security over WEP.

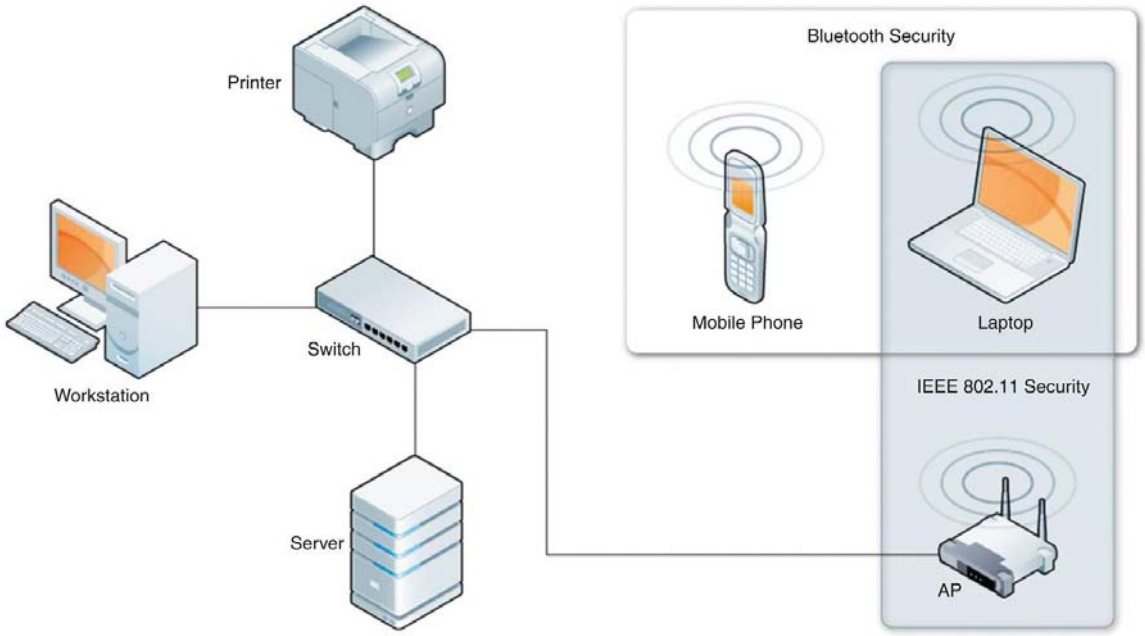


The major terms and security areas of focus include the following:

WPA: Initial WPA version, to supply enhanced security over the older WEP protocol. Typically uses the Temporal Key Integrity Protocol (TKIP) encryption protocol.
WPA2: Also known as IEEE 802.11i-2004. Successor of WPA, and replaces the TKIP encryption protocol with Counter Cipher Mode with Block Chaining Message Authentication Protocol (CCMP) to provide additional security.
TKIP: A 128-bit per-packet key is used, meaning that it dynamically generates a new key for each packet. This is part of the IEEE 802.11i standard. TKIP implements per-packet key mixing with a rekeying system and also provides a message integrity check. These avoid the problems of WEP.
CCMP: An AES-based encryption mechanism that is stronger than TKIP; sometimes referred to as AES instead of CCMP.
EAP: Extensible Authentication Protocol. EAP is an authentication framework providing for the transport and usage of keying material and parameters generated by EAP methods since EAP uses a central authentication server.
WPA-Personal: Also referred to as WPA-preshared key (PSK) mode. Is designed for home and small office networks and does not require an authentication server. Each wireless network device authenticates with the AP using the same 256-bit key.
WPA-Enterprise: Also referred to as WPA-802.1X mode, and sometimes just WPA (as opposed to WPA-PSK). Is designed for enterprise networks, and requires a Remote Authentication Dial-In User Server (RADIUS) authentication server.

This requires a more complicated setup, but provides additional security (e.g., protection against dictionary attacks). An EAP is used for authentication, which comes in different flavors (e.g., EAP-TLS, EAP-Tunneled Transport Layer Security (TTLS), EAP-security information management (SIM)).

Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances.



Bluetooth wireless

Cumulatively, the various versions of Bluetooth specifications define four security modes. Each version of Bluetooth supports some, but not all, of the four modes. Each Bluetooth device must operate in one of the four modes, which are described below.

Security Mode 1 is nonsecure. Security functionality (authentication and encryption) is bypassed, leaving the device and connections susceptible to attackers. In effect, Bluetooth devices in this mode are "promiscuous" and do not employ any mechanisms to prevent other Bluetooth-enabled devices from establishing connections. Security Mode 1 is supported only in v2.0 + enhanced data rate (EDR) (and earlier) devices.

In *Security Mode 2*, a service level-enforced security mode, security procedures are initiated after Link Management Protocol (LMP) link establishment but before Logical Link Control and Adaptation (L2CAP) channel establishment. L2CAP resides in the data link layer and provides connection-oriented and connectionless data services to upper layers. For this security mode, a security manager (as specified in the Bluetooth architecture) controls access to specific services and devices.

The centralized security manager maintains policies for AC and interfaces with other protocols and device users. Varying security policies and trust levels to restrict access may be defined for applications with different security requirements operating in parallel. It is possible to grant access to some services without providing access to other services. In this mode, the notion of authorization – the process of deciding if a specific device is allowed to have access to a specific service – is introduced.

In *Security Mode 3*, the link level-enforced security mode, a Bluetooth device initiates security procedures before the physical link is fully established. Bluetooth devices operating in Security Mode 3 mandate authentication and encryption for all connections to and from the device. This mode supports authentication (unidirectional or mutual) and encryption.

Similar to Security Mode 2, *Security Mode 4* (introduced in Bluetooth v2.1 + EDR) is a service level-enforced security mode in which security procedures are initiated after link setup. Security requirements for services protected by Security Mode 4 must be classified as one of the following: authenticated link key required, unauthenticated link key required, or no security required. Whether or not a link key is authenticated depends on the Secure Simple Pairing association model used.

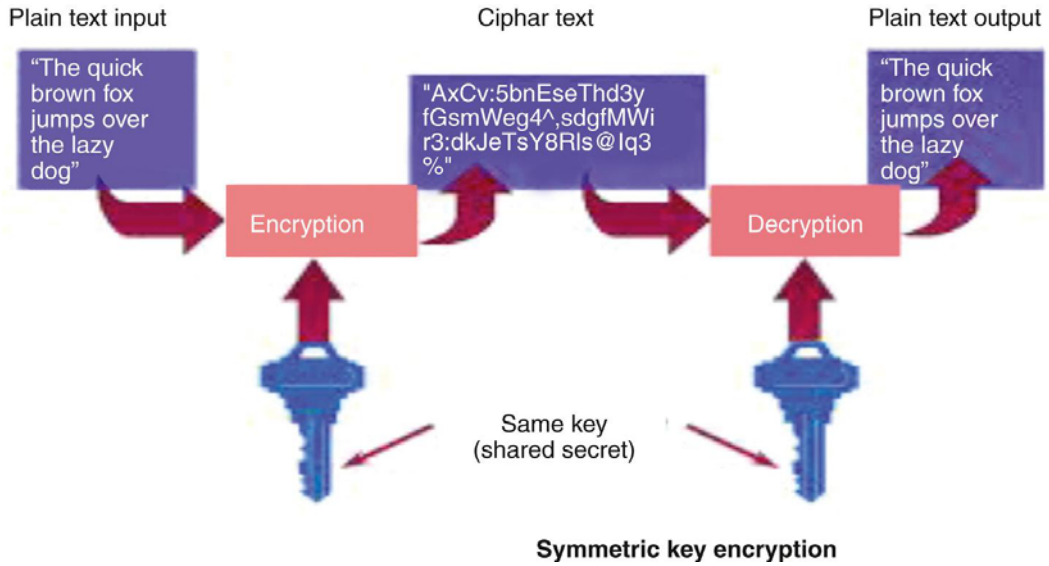
Cryptography

Three types of encryption as currently used in security controls:

1. *Symmetric*: One method of cryptography is *symmetric cryptography* (also known as *secret key cryptography* or *private key cryptography*). Symmetric cryptography is best suited for bulk encryption because it is much faster than asymmetric cryptography. With symmetric cryptography:

   a. Both parties share the *same* key (which is kept secret). Before communications begin, both parties must exchange the shared secret key. Each pair of communicating entities requires a unique shared key. The key is not shared with other communication partners.

Note: Other names – secret key, conventional key, session key, file encryption key, etc.



Symmetric key encryption

Pros:

a. Speed/file size:

- Symmetric-key algorithms are generally much less computationally intensive which provides a smaller file size that allows for faster transmissions and less storage space.

Cons:

a. Key management:

- One disadvantage of symmetric-key algorithms is the requirement of a *shared secret key*, with one copy at each end. See drawing below.
- In order to ensure secure communications between everyone in a population of n people a total of $n(n-1)/2$ keys are needed. Example: key for 10 individuals, $10(10-1)/2 = 45$ keys.
- The process of selecting, distributing, and storing keys is known as key management; it is difficult to achieve reliably and securely.

Symmetric

Symmetric cryptography has an equation of $n\times(n-1)/2$ for the number of keys needed. In a situation with 1000 users, that would mean *499,500 keys*.

Asymmetric

Asymmetric cryptography, using key pairs for each of its users, has *n* as the number of key pairs needed. In a situation with 1000 users, that would mean *1000 key pairs*.

Symmetric algorithms:

Methods	Characteristics
Data Encryption Standard (DES)	• Created in 1972 and recertified in 1993 • Uses a 64-bit block size and a 56-bit key • Can be easily broken
Triple DES (3DES)	• Applies DES three times. Uses a 168-bit key • Replaced with AES

(*Continued*)

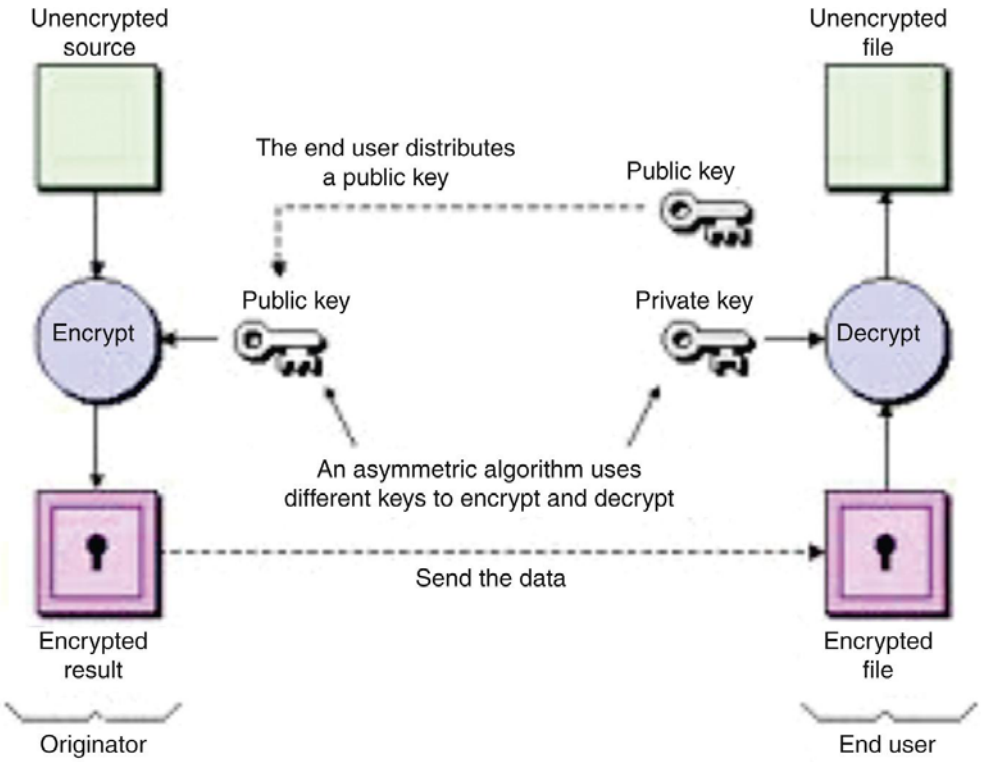
Methods	Characteristics
Advanced Encryption Standard (AES)	• Uses the Rijndael block cipher (rhine-doll) which is resistant to all known attacks • Uses a variable-length block and key length (128-, 192-, or 256-bit keys)
Blowfish	• Variable block size, variable key size (up to 448 bits)
Twofish	• Uses 128-bit blocks and variable key lengths (128-, 192-, or 256 bits)
Carlisle Adams Stafford Tavares (CAST)	• Two implementations: 64-bit block size with 128-bit key, 128-bit block size with 256-bit key. Used by Pretty Good Privacy (PGP) email encryption
International Data Encryption Algorithm (IDEA)	• Two implementations: 64-bit block size with 128-bit key, 128-bit block size with 256-bit key. Used by PGP email encryption

Rivest	• Includes various implementations:
	  • RC2 with 64-bit blocks and a variable key length (any size)
	  • RC4 with 40- and 128-bit keys
	  • RC5 with variable blocks and keys (any size)
	  • RC6 an improvement on RC5

2. *Asymmetric*: *Asymmetric* cryptography is a second form of cryptography. It is scalable for use in very large and ever expanding environments where data is frequently exchanged between different communication partners. With asymmetric cryptography:

a. Each user has two keys: a *public* key and a *private* key.
b. Both keys are mathematically related (both keys together are called the *key pair*).
c. The public key is made available to anyone. The private key is kept secret.
d. Both keys are required to perform an operation. For example, data encrypted with the private key is unencrypted with the *public* key. Data encrypted with the public key is unencrypted with the *private* key.
e. Encrypting data with the private key creates a digital *signature*. This ensures the message has come from the stated sender (because only the sender had access to the private key to be able to create the signature).
f. A digital envelope is signing a message with a recipient's public key. A digital *envelope*, which serves as a means of AC by ensuring that only the intended recipient can open the message (because only the receiver will have the private key necessary to unlock the envelope; this is also known as *receiver authentication*).
g. If the private key is ever discovered, a new key pair must be generated.

Asymmetric cryptography is often used to exchange the secret key to prepare for using symmetric cryptography to encrypt data. In the case of a key exchange, one party creates the secret key and encrypts it with the public key of the recipient. The recipient would then decrypt it with their private key. The remaining communication would be done with the secret key being the encryption key. Asymmetric encryption is used in key exchange, email security, web security, and other encryption systems that require key exchange over the public network.



Asymmetric key encryption

Pros:

a. Key management:
- Two keys (public and private), private key cannot be derived for the public so the public key can be freely distributed without confidentially being compromised
- Offers digital signatures, integrity checks, and nonrepudiation

Cons:

a. Speed/file size:
- Because symmetric-key algorithms are generally much less computationally intensive than asymmetric-key algorithms.
- In practice, asymmetric-key algorithm are typically hundreds to thousands times slower than a symmetric-key algorithm.

Asymmetric algorithms:

Method	Characteristics
Rivest–Shamir–Adleman (RSA)	• Uses a specific one-way function based on the difficulty of factoring *N*, a product of 2 large prime numbers (200 digits)

Diffie–Hellman key exchange	• Known as a *key exchange algorithm*
	• Uses two system parameters (*p* and *g*)
	  • *p* is a prime number
	  • *g* is an integer smaller than *p* generated by both parties

(*Continued*)

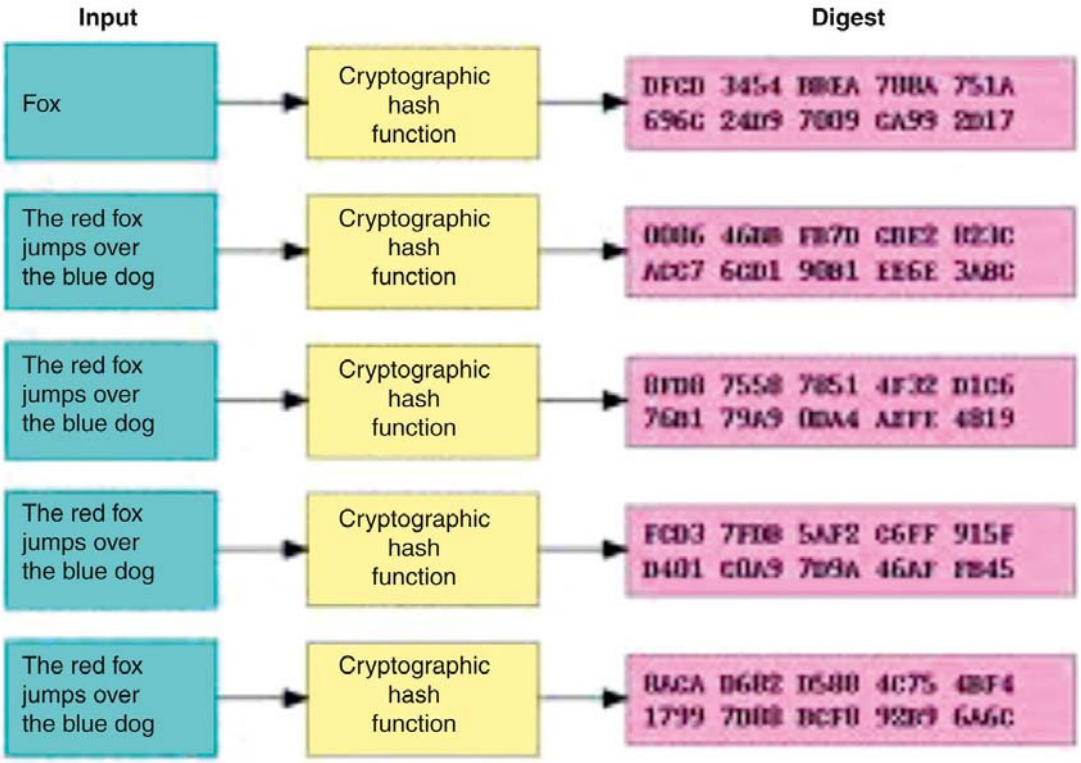
Method	Characteristics
ElGamal	• Extends Diffie–Hellman for use in encryption and digital signatures
Elliptic curve (EC)	• Used in conjunction with other methods to reduce the key size • An EC key of 160 bits is equivalent to 1024-bit RSA key, which means less computational power and memory requirements • Suitable for hardware applications (e.g., smart cards and wireless devices)
Digital Signature Algorithm (DSA)	• Used to digital sign documents • Performs integrity check by use of SHA hashing

3. *Hashing*: A *hash* is a function that takes a variable-length string (message), and compresses and transforms it into a fixed-length value.
   - **a.** The hashing algorithm (formula or method) is public.
   - **b.** Hashing uses a secret value to protect the method.
   - **c.** Hashing is used to create checksums or message digests (e.g., an investigator can create a checksum to secure a removable media device that is to be used as evidence).
   - **d.** The hash ensures data integrity (i.e., the data have not been altered). The receiving device computes a checksum and compares it to the checksum included with the file. If they do not match, the data has been altered.
   - **e.** Examples include message digest (MD2, MD4, MD5) and Secure Hashing Algorithm (SHA).
   - **f.** SHA, Race Integrity Primitives Evaluation Message Digest (RIPEMD), and Hash of Variable Length (HAVAL).

Name	Class	Hash length
MD5	*512-Bit blocks*	*Digest size(s)*: 128 bits *Rounds*: 4
SHA-1	*512-Bit blocks*	*Digest size(s)*: 160 bits *Rounds*: 80
SHA-2 SHA-224/256	*512-Bit blocks*	*Digest size(s)*: 256 bits *Rounds*: 64
SHA-2 SHA-384/512	1024-Bit blocks	*Digest size(s)*: 512 bits *Rounds*: 80
RIPEMD-160		*Digest size(s)*: 128,160, 256, and 320 bits
HAVAL		*Digest size(s)*: 128, 160, 192, 224, and 256 bits *Rounds*: 3, 4, or 5

Secure Hash

The secure hash function takes a stream of data and reduces it to a fixed size through a one-way mathematical function. The result is called a message digest and can be thought of as a fingerprint of the data. The message digest can be reproduced by any party with the same stream of data, but it is virtually impossible to create a different stream of data that produces the same message digest.



Secure Hash Standard

The Secure Hash Standard specifies five SHAs: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. All five of the algorithms are iterative, one-way hash functions that can process a message to produce a condensed representation called a *message digest*. These algorithms enable the determination of a message's integrity: any change to the message will, with a very high probability, result in a different message digest. This property is useful in the generation and verification of digital signatures and MACs, and in the generation of random numbers or bits.

The five algorithms differ most significantly in the security strengths that are provided for the data being hashed. The security strengths of these five hash functions and the system as a whole when each of them is used with other cryptographic algorithms, such as Digital Signature Algorithms (DSAs) and keyed-hash MACs, can be found in SP 800-57 and SP 800-107.

Additionally, the five algorithms differ in terms of the size of the blocks and words of data that are used during hashing.

HMAC

Providing a way to check the integrity of information transmitted over or stored in an unreliable medium is a prime necessity in the world of open computing and communications. Mechanisms that provide such integrity checks based on a secret key are usually called MACs. Typically, MACs are used between two parties that share a secret key in order to authenticate

information transmitted between these parties. This standard defines a MAC that uses a cryptographic hash function in conjunction with a secret key. This mechanism is called Hash-Based Message Authentication Code (HMAC). HMAC shall use an approved cryptographic hash function [FIPS-180-3]. It uses the secret key for the calculation and verification of the MACs.

So, in review, the table below covers the three types of encryption and their particular uses:

- Encryption provides confidentiality.
- Hashing provides integrity (like a checksum).
- Digital signatures provide authentication and integrity.
- Digitally signed encryption provides confidentiality, authentication, and integrity.

Mechanism		Data integrity	Confidentiality	Identification and authentication	Nonrepudiation	Key distribution
Symmetric-key cryptography	Encryption	No	Yes	No	No	No
	Message authentication codes	Yes	No	Yes	No	No
	Key transport	No	No	No	No	Yes – requires out-of-band initialization step or a TTP
Secure hash functions	Message digest	Yes	No	No	No	No
	HMAC	Yes	No	Yes	No	No
Asymmetric cryptography	Digital signatures	Yes	No	Yes	Yes (with a TTP)	No
	Key transport	No	No	No	No	Yes
	Key agreement	No	No	Yes	No	Yes

Intrusion Detection Systems

Another element to securing networks complementing firewall implementations is an IDS. An IDS works in conjunction with routers and firewalls by monitoring network usage anomalies by being deployed in a demilitarized zone (DMZ) on the edge of the network or it is utilized as a network-based device inside the network to monitor for specific traffic patterns and alert when these patterns are identified so it protects a company's information system resources from external as well as internal misuse.

An IDS operates continuously on the system, running in the background and notifying administrators when it detects a perceived threat. For example, an IDS detects attack patterns and issues an alert. Broad categories of IDS include:

- *Network-based IDSs*: Identify attacks within the monitored network and issue a warning to the operator. If a network-based IDS is placed between the internet and the firewall, it will detect all the attack attempts, whether or not they enter the firewall. If the IDS is placed between a firewall and the corporate network, it will detect those attacks that

enter the firewall (it will detect intruders). The IDS is not a substitute for a firewall, but it complements the function of a firewall.

- *Host-based IDSs*: Configured for a specific environment and will monitor various internal resources of the operating system to warn of a possible attack. They can detect the modification of executable programs, detect the deletion of files, and issue a warning when an attempt is made to use a privileged command.

Common Intrusion Detection Methodologies

- Signature-Based Detection
  A *signature* is a pattern that corresponds to a known threat. *Signature-based detection* is the process of comparing signatures against observed events to identify possible incidents. 5 Examples of signatures are as follows:
  A telnet attempt with a username of "root", which is a violation of an organization's security policy.
  An email with a subject of "Free pictures!" and an attachment filename of "freepics.exe", which are characteristics of a known form of malware.
  An operating system log entry with a status code value of 645, which indicates that the host's auditing has been disabled.
  Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats, threats disguised by the use of evasion techniques, and many variants of known threats.
- Anomaly-Based Detection
  Anomaly-based detection is the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. An IDPS using anomaly-based detection has *profiles* that represent the normal behavior of such things as users, hosts, network connections, or applications. The profiles are developed by monitoring the characteristics of typical activity over a period of time. The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown threats.
- Stateful Protocol Analysis
  Stateful protocol analysis is the process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Unlike anomaly-based detection, which uses host or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. The "stateful" in stateful protocol analysis means that the IDPS is capable of understanding and tracking the state of network, transport, and application protocols that have a notion of state.
  Stateful protocol analysis can identify unexpected sequences of commands, such as issuing the same command repeatedly or issuing a command without first issuing a command upon which it is dependent. Another state tracking feature of stateful protocol analysis is that for protocols that perform authentication, the IDPS can keep track of the authenticator used for each session, and record the authenticator used for suspicious activity. This is helpful when investigating an incident. Some IDPSs can also use the authenticator information to define acceptable activity differently for multiple classes of users or specific users.
  The "protocol analysis" performed by stateful protocol analysis methods usually includes reasonableness checks for individual commands, such as minimum and maximum lengths for arguments. If a command typically has a username argument, and usernames have a maximum length of 20 characters, then an argument with a length of 1000 characters is suspicious. If the large argument contains binary data, then it is even more suspicious.[28]

Types of IDSs include:

- *Signature-based*: These IDS systems protect against detected intrusion patterns. The intrusive patterns they can identify are stored in the form of signatures.

[28]SP 800-94, p. 2-4 to 2-6.

- *Statistical-based*: These IDS systems need a comprehensive definition of the known and expected behavior of systems.
- *Neural networks*: An IDS with this feature monitors the general patterns of activity and traffic on the network and creates a database. This is similar to the statistical model but with added self-learning functionality.

Signature-based IDSs will not be able to detect all types of intrusions due to the limitations of the detection rules. On the other hand, statistical-based systems may report many events outside of defined normal activity but which are normal activities on the network. A combination of signature- and statistical-based models provides better protection.

Uses of IDPS Technologies

- Identifying possible incidents
- Identifying reconnaissance activity
- Identifying security policy problems
- Documenting existing threat to an organization
- Deterring individuals from violating security policies

The table below is a high-level comparison of the four primary IDPS technology types. The strengths listed in the table indicate the roles or situations in which each technology type is generally superior to the others. A particular technology type may have additional benefits over others, such as logging additional data that would be useful for validating alerts recorded by other IDPSs, or preventing intrusions that other IDPSs cannot because of technology capabilities or placement.[29]

IDPS Technology Type	Types of Malicious Activity Detected	Scope per Sensor or Agent	Strengths
Network-Based	Network, transport, and application TCP/IP layer activity	Multiple network subnets and groups of hosts	Able to analyze the widest range of application protocols; only IDPS that can thoroughly analyze many of them
Wireless	Wireless protocol activity; unauthorized wireless local area networks (WLAN) in use	Multiple WU\Ns and groups of wireless clients	Only IDPS that can monitor wireless protocol activity
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows	Multiple network subnets and groups of hosts	Typically more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing major malware infections
Host-Based	Host application and operating system (OS) activity; network, transport, and application TCP/IP layer activity	Individual host	Only IDPS that can analyze activity that was transferred in end-to-end encrypted communications

[29]SP 800-94, p. 8-1.

Key areas which the assessor should focus on when reviewing and evaluating IDS deployments include:

- Recording information related to observed events
- Notifying security administrators of important observed events
- Producing reports
- Response techniques:
  - Stops attack
  - Changes security environment
  - Changes attack's content
- False-positive adjustments
- False-negative adjustments
- Tuning
- Evasion

FIREWALLS

Firewall Security Systems – SP 800-41

Every time a corporation connects its internal computer network to the internet it faces potential danger. Because of the internet's openness, every corporate network connected to it is vulnerable to attack. Hackers on the internet could theoretically break into the corporate network and do harm in a number of ways: steal or damage important data, damage individual computers or the entire network, use the corporate computer's resources, or use the corporate network and resources as a way of posing as a corporate employee. Companies should build firewalls as one means of perimeter security for their networks. Likewise, this same principle holds true for very sensitive or critical systems that need to be protected from untrusted users inside the corporate network (internal hackers). Firewalls are defined as a device installed at the point where network connections enter a site; they apply rules to control the type of networking traffic flowing in and out. Most commercial firewalls are built to handle the most commonly used internet protocols.

To be effective, firewalls should allow individuals on the corporate network to access the internet and, at the same time, stop hackers or others on the internet from gaining access to the corporate network to cause damage. Generally, most organizations will follow a deny-all philosophy, which means that access to a given resource will be denied unless a user can provide a specific business reason or need for access to the information resource. The converse of this access philosophy, not widely accepted, is the accept-all philosophy under which everyone is allowed access unless someone can provide a reason for denying access.

Firewall General Features

Firewalls are hardware and software combinations that are built using routers, servers, and a variety of software. They should control the most vulnerable point between a corporate network and the internet, and they can be as simple or complex as the corporate

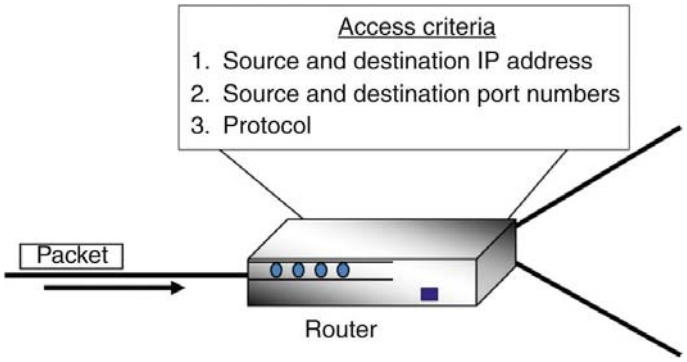
information security policy demands. There are many different types of firewalls, but most enable organizations to:

- Block access to particular sites on the internet
- Limit traffic on an organization's public services segment to relevant addresses and ports
- Prevent certain users from accessing certain servers or services
- Monitor communications between an internal and an external network
- Monitor and record all communications between an internal network and the outside world to investigate network penetrations or detect internal subversion
- Encrypt packets that are sent between different physical locations within an organization by creating a VPN over the internet (i.e., IPSec VPN tunnels)

Firewall Types

Generally, the types of firewalls available today fall into four categories which include:

- *Packet filtering*: *Packet filtering* is a security method of controlling what data can flow to and from a network. It takes place by using Access Control Lists (ACLs), which are developed and applied to a device. The ACL is just lines of text, called rules, which the device will apply to each packet that it receives. The lines of text give specific information pertaining to what packets can be accepted and what packets are denied. For instance, an ACL can have one line that states that any packets coming from the IP range 172.168.0.0 must be denied. Another line may indicate that no packets using the FTP service will be allowed to enter the network, and another line may indicate that no traffic is to be allowed through port 443. Then it can have a line indicating all traffic on port 80 is acceptable and should be routed to a specific IP address, which is the web server. Each time the device receives a packet, it compares the information in the packet's header to each line in the ACL. If the packet indicates it is using FTP or requests to make a connection to the 443 port, it is discarded. If the packet header information indicates that it wants to communicate through port 80 using HTTP over TCP, then the packet is accepted and redirected to the web server.



This filtering is based on network layer information, which means that the device cannot look too far into the packet itself. It can make decisions based on only header information,

which is limited. Most routers use ACLs to act as a type of router and to carry out routing decisions, but they do not provide the level of protection that other types of firewalls, which look deeper into the packet, provide. Since packet filtering looks only at the header information, it is not application dependent like many proxy firewalls are. Packet filtering firewalls do not keep track of the state of a connection, which takes place in a stateful firewall.

Pros:

- Scalable
- Provides high performance
- Application independent

Cons:

- Does not look into the packet past the header information
- *Low security relative to other options*
- *Does not keep track of the state of a connection*

Note: *Packet filtering cannot protect against mail bomb attacks because it cannot read the content of the packet.*

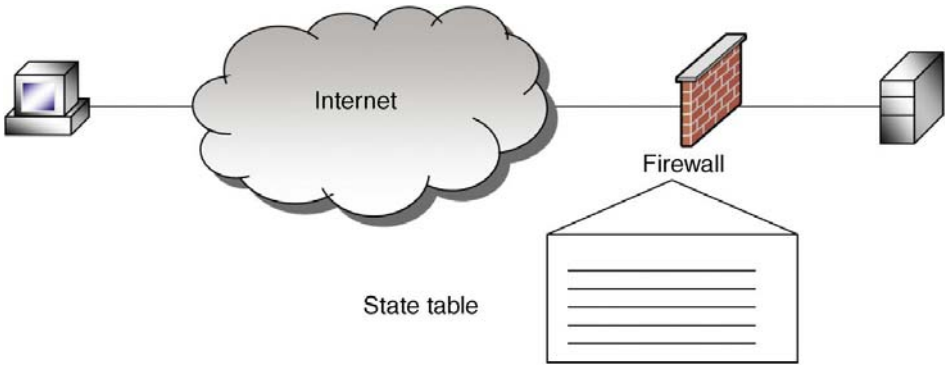
- *Application firewall systems*: *Application-level firewalls* inspect the entire packet and make access decisions based on the actual content of the packet. They understand different services and protocols and the commands that are used within them. An application-level proxy can distinguish between an FTP GET command and an FTP PUT command and make access decisions based on this granular level of information, where packet filtering firewalls can only allow or deny FTP requests as a whole, not the commands used within the FTP protocol.

  An application-level firewall works for one service or protocol. A computer can have many different types of services and protocols (FTP, Network Time Protocol (NTP), Simple Mail Transfer Protocol (SMTP), Telnet, etc.); thus, there must be one application-level proxy per service. Providing application-level proxy services can be much trickier than it appears. The proxy must totally understand how specific protocols work and what commands within that protocol are legitimate. This is a lot to know and look at during the transmission of data. If the application-level proxy firewall does not understand a certain protocol or service, it cannot protect this type of communication. This is when a circuit-level proxy can come into play because it does not deal with such complex issues. An advantage of circuit-level proxies is that they can handle a wider variety of protocols and services than application-level proxies, but the downfall is that the circuit-level proxy cannot provide the degree of granular control that an application-level proxy can. Life is just full of compromises.

  So, an application-level firewall is dedicated to a particular protocol or service. There must be one proxy per protocol because one proxy could not properly interpret all the commands of all the protocols coming its way. A circuit-level proxy works at a lower layer of the Open Systems Interconnection (OSI) model and does not require one proxy per protocol because it is not looking at such detailed information.

- *Stateful inspection*: When regular packet filtering is used, a packet arrives at the router, and the router runs through its ACLs to see if this packet should be allowed or denied. If the packet is allowed, it is passed on to the destination host or another router, and the router forgets it ever received this packet. This is different from stateful filtering, which remembers what packets went where until that particular connection is closed. Stateful routers also make decisions on what packets to allow or disallow, but their logic goes a step farther. For example, a regular packet filtering device may deny any UDP packets requesting service on port 25, and a stateful filtering device may have the rule to allow UDP packets through only if they are responses to outgoing requests. Basically, the stateful firewall will want to allow only those packets in that its internal hosts requested.

  If User A sends a request to a computer on a different network, this request will be logged in the firewall's state table. The table will indicate that User A's computer made a request and there should be packets coming back to User A. When the computer on the internet responds to User A, these packets will be compared to data in the state table. Since the state table does have information about a previous request for these packets, the router will allow the packets to pass through. If, on the other hand, User A did not make any requests and packets were coming in from the internet to him, the firewall will see that there were no previous requests for this information and then look at its ACLs to see if these packets are allowed to come in.



So, regular packet filtering compares incoming packets to rules defined in its ACLs. When stateful packet filtering receives a packet, it first looks in its state table to see if a connection has already been established and if this data was requested. If there is no previous connection and the state table holds no information about the packets, the packet is compared to the device's ACLs. If the ACL allows this type of traffic, the packet is allowed to access the network. If that type of traffic is not allowed, the packet is dropped. Although this provides an extra step of protection, it also adds more complexity because this device must now keep a dynamic state table and remember connections. This has opened the door to many types of denial-of-service attacks. There are several types of attacks that are aimed at flooding the state table with bogus information. The state table is a resource like a system's hard drive space, memory, and CPU. When the state table is stuffed full of bogus information, it can either freeze the device or cause it to

reboot. Also, if this firewall has to be rebooted for some reason, it loses its information on all recent connections; thus, it will deny legitimate packets.

Note: Context AC pertains to a sequence of events proceeding the access request and specifics of the environment within a window of time. Content pertains to making an AC decision based on the data being protected.

- A stateful firewall is a context AC.
- Fourth-generation firewall = dynamic packet filter.
- Fifth-generation firewall = kernel proxies.

- *Circuit or application proxy*: A *proxy* is a middleman. If someone needed to give a box and a message to the President of the United States, this person could not just walk up to him and give him these items. The person would have to go through a middleman who would accept the box and message and thoroughly go through the box to ensure nothing dangerous was inside. This is what a proxy firewall does: it accepts messages either entering or leaving a network, inspects them for malicious information, and, when it decides things are okay, passes the data on to the destination computer.

  A proxy will stand between a trusted and untrusted network and will actually make the connection, each way, on behalf of the source. So if a user on the internet requests to send data to a computer on the internal, protected network, the proxy will get this request and look it over for suspicious information. The request does not automatically go to the destination computer; the proxy server acts like the destination computer. If the proxy decides the packet is safe, it sends it on to the destination computer. When the destination computer replies, the reply goes back to the proxy server, who repackages the packet to contain the source address of the proxy server, not the host system on the internal network. All external connections heading to the internal network are terminated at the proxy server. This type of firewall makes a copy of each accepted packet before transmitting it. It will repackage the packet to hide the packet's true origin.

  Just like the packet filtering firewalls, proxy firewalls also have a list of rules that are applied to packets. When the proxy firewall receives a packet, it runs through this list of rules to see if the packet should be allowed. If the packet is allowed, the proxy firewall repackages the packet and sends it on its way to the destination computer. When users go through a proxy, they do not usually know it. Users on the internet think they are talking directly to users on the internal network and vice versa. The proxy server is the only machine that talks to the outside world. This ensures that no computer has direct access to internal computers. This also means that the proxy server is the only computer that needs a valid IP address. The rest of the computers on the internal network can use private (nonroutable IP addresses on the internet) addresses, since no computers on the outside will see their addresses anyway.

  Many times, proxy servers are used when a company is using a *dual-homed firewall*. A dual-homed firewall has two interfaces: one facing the external network and the other facing the internal network. This is different than a computer that has forwarding enabled, which just lets packets pass through its interfaces with no AC enforced. A dual-homed firewall has two network interface cards (NICs) and should have packet forwarding and routing turned off. They are turned off for safety reasons. If forwarding were enabled, the computer would not apply the necessary ACL rules or other restrictions necessary of a firewall. Instead, a dual-homed firewall requires a higher

level of intelligence to tell it what packets should go where and what types of packets are acceptable. This is where the proxy comes in. When a packet comes to the external NIC from the untrusted network on a dual-homed firewall, the computer does not know what to do with it, so it passes it up to the proxy software. The proxy software inspects the packet to make sure that it is legitimate. Then the proxy software makes a connection with the destination computer on the internal network and passes on the packet. When the internal computer replies, the packet goes to the internal interface on the dual-homed firewall, it passes up to the proxy software, the proxy inspects the packet and slaps on a different header, and the proxy passes the packet out the external NIC that is connected to the external network.

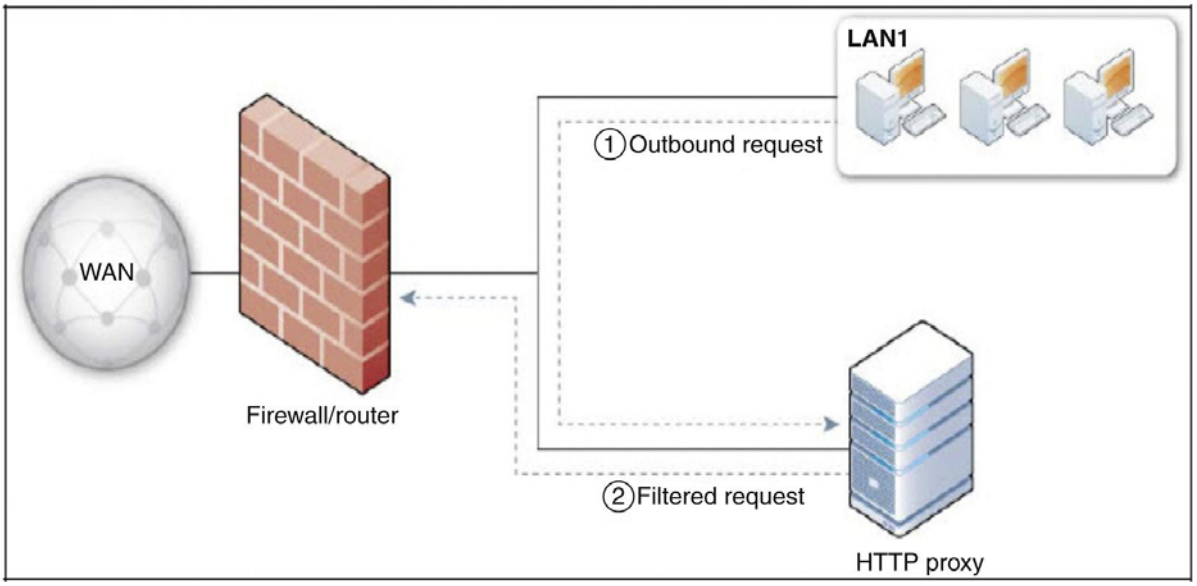
Pros:

- Looks at the information within a packet all the way up to the application layer
- Provides better security than packet filtering
- Breaks the connection between trusted and untrusted systems

Cons:

- Some proxy firewalls are limited to what applications they can support.
- Degrades traffic performance.
- Poor scalability for application-based proxy firewalls.

Note: Breaks client/server model – which is good for security, but at times bad for functionality.



Firewall Utilization

- Most companies have firewalls to restrict access into their network from internet users. They may also have firewalls to restrict one internal network from accessing another internal network. An organizational security policy will give high-level instructions

on acceptable and unacceptable actions as they pertain to security. The firewall will have a more defined and granular security policy that dictates what services are allowed to be accessed, what IP addresses and ranges are to be restricted, and what ports can be accessed. The firewall is described as a "choke point" in the network, since all communication should flow through it and this is where traffic is inspected and restricted. A firewall is actually a type of gateway that can be a router, server, authentication server, or specialized hardware device. It monitors packets coming into and out of the network it is protecting. It filters out the packets that do not meet the requirements of the security policy. It can discard these packets, repackage them, or redirect them depending on the firewall configuration and security policy. Packets are filtered based on their source and destination addresses and ports, by service, packet type, protocol type, header information, sequence bits, and much more. Each vendor has different functionality and different parameters they can use for identification and access restriction.

Examples of Firewall Implementations

Firewall implementations can take advantage of the functionality available in a variety of firewall designs to provide a robust layered approach in protecting an organization's information assets. Commonly used implementations available today include:

- *Screened-host firewall*: Utilizing a packet filtering router and a bastion host, this approach implements basic network layer security (packet filtering) and application server security (proxy services). An intruder in this configuration has to penetrate two separate systems before the security of the private network can be compromised. This firewall system is configured with the bastion host connected to the private network with a packet filtering router between the internet and the bastion host. Router filtering rules allow inbound traffic to access only the bastion host, which blocks access to internal systems. Since the inside hosts reside on the same network as the bastion host, the security policy of the organization determines whether inside systems are permitted direct access to the internet, or whether they are required to use the proxy services on the bastion host.
- *Dual-homed firewall*: A firewall system that has two or more network interfaces, each of which is connected to a different network. In a firewall configuration, a dual-homed firewall usually acts to block or filter some or all of the traffic trying to pass between the networks. A dual-homed firewall system is a more restrictive form of a screened-host firewall system, when a dual-homed bastion host is configured with one interface established for information servers and another for private network host computers.
- *DMZ or screened-subnet firewall*: Utilizing two packet filtering routers and a bastion host, this approach creates the most secure firewall system, since it supports both network and application-level security while defining a separate DMZ network. The DMZ functions as a small isolated network for an organization's public servers, bastion host information servers and modem pools. Typically, DMZs are configured to limit access from the internet and the organization's private network. Incoming traffic access is restricted into the DMZ network by the outside router and protects the organization against certain attacks by limiting the services available for use. Consequently, external systems can

access only the bastion host (and its proxy service capabilities to internal systems) and possibly information servers in the DMZ. The inside router provides a second line of defense, managing DMZ access to the private network, while accepting only traffic originating from the bastion host. For outbound traffic, the inside router manages private network access to the DMZ network. It permits internal systems to access only the bastion host and information servers in the DMZ. The filtering rules on the outside router require the use of proxy services by accepting only outbound traffic on the bastion host. The key benefits of this system are that an intruder must penetrate three separate devices, private network addresses are not disclosed to the internet, and internal systems do not have direct access to the internet.

Note: In UNIX systems, the product TCP Wrappers can be used as a personal firewall or host-based IDS.

The assessor should review and test the following areas when conducting a comprehensive evaluation of the firewall and its technology:

- Scanning firewall from the outside and inside
- Scanning with firewall down to see level of exposure if it went off-line
- Directional control
- Incoming packet with internal source address
- Outgoing packet with external source address
- FTP out but not in
- Making sure that access to the firewall is authorized
- How are employees and nonemployees given access
- Obtaining a list of users on the firewall
- Cross-checking with staff lists/organization chart
- Remote administration:
  - One-time passwords
  - Other secure methods
  - Encrypted link
- How is access changed or revoked
- How is access reviewed:
  - Mechanics of authentication
  - Frequency of review
  - Password reset/changing passwords
  - Root password control
- Need for firewall to enforce security policy (encryption, viruses, URL blocks, proxy/packet filter types of traffic):
  - The rule set obtained?
  - How are rule sets stored to maintained to ensure that they have not been tampered with?
  - Checksums regularly verified?
- Determining whether the effectiveness of firewall has been tested
- Reviewing processes running on firewall; are they appropriate:
  - Does the firewall provide adequate notice when an exploit is attempted?

AUDIT AND ACCOUNTING

Most, if not all, of the guidance for the audit and accountability family of controls can be found in the SP 800-92, *Guide to Log Management*.

Log Management

A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security. These computer security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; and applications. Logs are emitted by network devices, operating systems, applications, and all manner of intelligent or programmable devices. A stream of messages in time sequence often comprises the entries in a log. Logs may be directed to files and stored on disk, or directed as a network stream to a log collector. Log messages must usually be interpreted with respect to the internal state of its source (e.g., application) and announce security-relevant or operations-relevant events (e.g., a user log-in, or a systems error).

A fundamental problem with log management that occurs in many organizations is effectively balancing a limited quantity of log management resources with a continuous supply of log data. Log generation and storage can be complicated by several factors, including a high number of log sources; inconsistent log content, formats, and timestamps among sources; and increasingly large volumes of log data. Log management also involves protecting the confidentiality, integrity, and availability of logs. Another problem with log management is ensuring that security, system, and network administrators regularly perform effective analysis of log data. This publication provides guidance for meeting these log management challenges.

Originally, logs were used primarily for troubleshooting problems, but logs now serve many functions within most organizations, such as optimizing system and network performance, recording the actions of users, and providing data useful for investigating malicious activity. Logs have evolved to contain information related to many different types of events occurring within networks and systems. Within an organization, many logs contain records related to computer security; common examples of these computer security logs are audit logs that track user authentication attempts and security device logs that record possible attacks.

The Special Publication 800-92 defines the criteria for logs, log management, and log maintenance in the following control areas:

- Auditable events
- Content of audit records
- Audit storage capacity
- Response to audit processing failures
- Audit review, analysis, and reporting
- Audit reduction and report generation
- Timestamps

- Audit record retention
- Audit generation

The SP defines the four parts of log management as follows:

1. Log management:
   a. Log sources.
   b. Analyze log data.
   c. Respond to identified events.
   d. Manage long-term log data storage.
2. Log sources:
   a. Log generation.
   b. Log storage and disposal.
   c. Log security.
3. Analyzing log data:
   a. Gain an understanding of logs.
   b. Prioritize log entries.
   c. Compare system-level and infrastructure-level analysis.
   d. Respond to identified events.
4. Manage long-term log data storage:
   a. Choose log format for data to be archived.
   b. Archive the log data.
   c. Verify integrity of transferred logs.
   d. Store media securely.

To address AU-10, nonrepudiation, the information system protects against an individual falsely denying having performed a particular action. Nonrepudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Nonrepudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

The Digital Signature Standard defines methods for digital signature generation that can be used for the protection of binary data (commonly called a message), and for the verification and validation of those digital signatures.

There are three techniques which are approved for this process:

1. The DSA is specified in this standard. The specification includes criteria for the generation of domain parameters, for the generation of public and private key pairs, and for the generation and verification of digital signatures.
2. The RSA DSA is specified in American National Standard (ANS) X9.31 and Public Key Cryptography Standard (PKCS) #1. FIPS-186-3 approves the use of implementations of either or both of these standards, but specifies additional requirements.
3. The Elliptic Curve Digital Signature Algorithm (ECDSA) is specified in ANS X9.62. FIPS-186-3 approves the use of ECDSA, but specifies additional requirements.

When assessing logs look for the following areas:

- Connections should be logged and monitored.

- What events are logged?
  - Inbound services
  - Outbound services
  - Access attempts that violate policy
- How frequent are logs monitored?
  - Differentiate from automated and manual procedures.
- Alarming:
  - Security breach response
  - Are the responsible parties experienced?
- Monitoring of privileged accounts

SIEM

Security information and event management (SIEM) is a term for software products and services combining SIM and security event management (SEM). The segment of security management that deals with real-time monitoring, correlation of events, notifications, and console views is commonly known as SEM. The second area provides long-term storage, analysis, and reporting of log data and is known as SIM.

SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. SIEM is sold as software, appliances, or managed services, and is also used to *log security data* and generate reports for compliance purposes. The term Security Information and Event Management (SIEM), coined by Mark Nicolett and Amrit Williams of Gartner in 2005, describes the product capabilities of gathering, analyzing, and presenting information from network and security devices; identity and access management applications; vulnerability management and policy compliance tools; operating system, database, and application logs; and external threat data. A key focus is to monitor and help manage user and service privileges, directory services, and other system configuration changes, as well as providing *log auditing and review* and IR.