NATIONAL UNIVERSITY
COLLEGE OF COMPUTING AND
INFORMATION TECHNOLOGIES

VER 1.0

COURSE MANUAL

INFORMATION ASSURANCE AND SECURITY

This course provides students with the theoretical knowledge and practical skills in the implementation of Information Assurance and Security providing relevant solutions for security hardening and information protection through computer vulnerability assessment, secure coding, and computer security hardening techniques.

BS – COMPUTER SCICENCE

BS – INFORMATION TECHNOLOGY

Security and System Administration Cluster

MODULE 3
PLANNING FOR SECURITY

Table of Contents

Lesson Topics

LESSON 1

Information Security Planning and Governance

Learning Outcomes:

- Understand the purpose and structure of security governance.
- Identify key governance roles and responsibilities.
- Align security strategies with business goals and risk appetite.
- Apply risk management to security planning.

Understanding Information Security Planning and Governance

An organization's information security effort succeeds only when it operates in conjunction with the organization's information security policy. An information security program begins with policy, standards, and practices, which are the foundation for the information security architecture and blueprint. The creation and maintenance of these elements require coordinated planning. The role of planning in modern organizations is hard to overemphasize. All but the smallest organizations engage in some planning: strategic planning to manage the allocation of resources and contingency planning to prepare for the uncertainties of the business environment.

Information Security Planning and Governance

Strategic planning sets the long-term direction to be taken by the organization and each of its component parts. Strategic planning should guide organizational efforts and focus resources toward specific, clearly defined **goals**. After an organization develops a general strategy, it generates an overall **strategic plan** (documented product of strategic planning) by extending that general strategy into plans for major divisions. Each level of each division then translates those plan **objectives** into more specific objectives for the level below. To execute this broad strategy, the executive team must first define individual responsibilities.

Planning Levels

Once the organization's overall strategic plan is translated into strategic plans for each major division or operation, the next step is to translate these plans into tactical objectives that move toward reaching specific, measurable, achievable, and time-bound accomplishments. The process of strategic planning seeks to transform broad, general, sweeping statements into more specific and applied objectives. Strategic plans are used to **create tactical plans**, which in turn are used to develop operational plans.

Tactical planning focuses on short-term undertakings that will be completed within one or two years. The process of tactical planning breaks each strategic goal into a series of incremental objectives. Each objective in a tactical plan should be specific and should have a delivery date within a year of the plan's start. Budgeting, resource allocation, and personnel are critical components of the tactical plan. Tactical plans often include project plans and resource acquisition planning documents (such as product specifications), project budgets, project reviews, and monthly and annual reports. The chief information security officer (CISO) and security managers use the tactical plan to organize, prioritize, and acquire resources necessary for major projects and to provide support for the overall strategic plan. Managers and employees use **operational planning** derived from tactical planning to organize the ongoing, day-today performance of tasks. An operational plan includes the necessary tasks for all relevant departments as well as communication and reporting requirements, which might include weekly meetings, progress reports, and other associated tasks. These plans must reflect the organizational structure, with each subunit, department, or project team conducting its own operational planning and reporting.

Information Security Governance

Governance describes the entire function of controlling, or governing, the processes used by a group to accomplish some objective. It represents the strategic controlling function of an organization's senior management, which is designed to ensure informed, prudent strategic decisions made in the best interest of the organization. Just like governments, corporations and other organizations have guiding documents—corporate charters or partnership agreements—as well as appointed or elected leaders or officers, and planning and operating procedures. These elements in combination provide corporate governance. Each operating unit within an organization also has controlling customs, processes, committees, and practices.

Information security governance then applies these principles and management structures to the information security function. The governance of information security is a strategic planning responsibility whose importance has grown in recent years. To secure information assets, management must integrate information security practices into the fabric of the organization, expanding corporate governance policies and controls to encompass the objectives of the information security process. Information security objectives must be addressed at the highest levels of an organization's management team in order to be effective and sustainable. A broader view of information security encompasses all of an organization's information assets, including the knowledge managed by those IT assets.

Understanding Information Security Policy, Standards, and Practices

Information Security Policy, Standards, and Practices

Policies function like laws in an organization because they dictate acceptable and unacceptable behavior there. Like laws, policies define what is right and wrong, the penalties for violating policy, and the appeal process. **Standards**, on the other hand, are more detailed statements of what must be done to comply with policy. They have the same requirements for compliance as policies. Standards may be informal or part of an organizational culture, as in **de facto standards**. Or, standards may be published, scrutinized, and ratified by a group, as in formal or **de jure standards**. Practices, procedures, and guidelines effectively explain how to comply with policy.

The meaning of the term security policy depends on the context in which it is used. Governmental agencies view security policy in terms of national security and national policies to deal with foreign states. A security policy can also communicate a credit card agency's method for processing credit card numbers. In general, a security policy is a set of rules that protects an organization's assets. An information security policy provides rules for protection of the organization's information assets.

Enterprise Information Security Policy

An **enterprise information security policy (EISP)** is also known as a general security policy, organizational security policy, IT security policy, or information security policy. The EISP is an executive-level document, usually drafted by or in cooperation with the organization's chief information officer.

The EISP guides the development, implementation, and management of the security program. It sets out the requirements that must be met by the information security blueprint or framework. It defines the purpose, scope, constraints, and applicability of the security program. Finally, it addresses legal compliance. According to NIST, the EISP typically addresses compliance in two areas:

1. General compliance to ensure that an organization meets the requirements for establishing a program and assigning responsibilities therein to various organizational components
2. The use of specified penalties and disciplinary action.

Issue-Specific Security Policy

In general, the **issue-specific security policy, or ISSP**,

1. addresses specific areas of technology as listed below,
    - E-mail
    - Use of the Internet and World WideWeb
    - Specific minimum configurations of computers to defend against worms and viruses
    - Prohibitions against hacking or testing organization security controls
    - Home use of company-owned computer equipment
    - Use of personal equipment on company networks (BYOD: bring your own device)
    - Use of telecommunications technologies, such as fax and phone
    - Use of photocopy equipment

    - Use of portable storage devices and any other device capable of storing digital files
    - Use of cloud-based storage services that are not self-hosted by the organization or engaged under contract
2. requires frequent updates, and
3. contains a statement about the organization's position on a specific issue.

Several approaches are used to create and manage ISSPs within an organization. Three of the most common are:

1. Independent ISSP documents, each tailored to a specific issue
2. A single comprehensive ISSP document that covers all issues
3. A modular ISSP document that unifies policy creation and administration while maintaining each specific issue's requirements

Systems-Specific Policy (SysSP)

While issue-specific policies are formalized as written documents readily identifiable as policy, **systems specific security policies (SysSPs)** sometimes have a different look. SysSPs often function as standards or procedures to be used when configuring or maintaining systems. For example, a SysSP might describe the configuration and operation of a network firewall. This document could include a statement of managerial intent; guidance to network engineers on the selection, configuration, and operation of firewalls; and an access control list that defines levels of access for each authorized user. SysSPs can be separated into two general groups, managerial guidance SysSPs and technical specifications SysSPs, or they can be combined into a single policy document that contains elements of both.

- **Managerial Guidance SysSPs** A managerial guidance SysSP document is created by management to guide the implementation and configuration of technology and to address the behavior of employees in ways that support information security.
- **Technical Specifications SysSPs** While a manager can work with a systems administrator to create managerial policy, as described in the preceding section, the systems administrator in turn might need to create a policy to implement the managerial policy. Each type of equipment requires its own set of policies, which are used to translate management's intent for the technical control into an enforceable technical approach. There are two general methods of implementing such technical controls: access control lists and configuration rules.

- **Access control lists (ACLs)** consist of details about user access and use permissions and privileges for an organizational asset or resource, such as a file storage system, software component, or network communications device. ACLs focus on assets and the users who can access and use them.
- **Configuration rules (or policies)** govern how a security system reacts to the data it receives. Rule-based policies are more specific to the operation of a system than ACLs, and they may or may not deal with users directly.
- **Combination SysSPs** in many organizations create a single document that combines the managerial guidance SysSP and the technical specifications SysSP.

Policy Management

Policies are living documents that must be managed and nurtured, and they are constantly changing and growing. These documents must be properly disseminated and managed. Special considerations should be made for organizations undergoing mergers, takeovers, and partnerships. In order to remain viable, these policies must have:

1. An individual responsible for reviews. The policy manager is often called the policy administrator. Note that the **policy administrator** does not necessarily have to be proficient in the relevant technology. While practicing information security professionals require extensive technical knowledge, policy management and policy administration require only a moderate technical background
2. A schedule of reviews. Policies can only retain their effectiveness in a changing environment if they are periodically reviewed for currency and accuracy and then modified accordingly. Policies that are not kept current can become liabilities as outdated rules are enforced (or not) and new requirements are ignored.
3. A method for making recommendations for reviews. To facilitate policy reviews, the policy manager should implement a mechanism by which people can comfortably make recommendations for revisions, whether via e-mail, office mail, or an anonymous drop box. If the policy is controversial, anonymous submission of recommendations may be the best way to encourage staff opinions.

4. An indication of policy and revision date. The simple action of dating the policy is often omitted. When policies are drafted and published without dates, confusion can arise. If policies are not reviewed and kept current, or if members of the organization are following undated versions, disastrous results and legal headaches can ensue. Such problems are particularly common in a high-turnover environment. Therefore, the policy must contain the date of origin and the date(s) of any revisions.

Automated Policy Management

There is an emergence of a new category of software for managing information security policies. In recent years, this category has emerged in response to needs articulated by information security practitioners. While there have been many software products that meet specific technical control needs, there is now a need for software to automate some of the busywork of policy management.

LESSON 2

The Information Security Blueprint

Learning Outcomes:

- Understand the role of a security blueprint in program development.
- Use common security architecture frameworks.
- Understand the design of security architecture.

Understanding Information Security Blueprint

The Information Security Blueprint

Once an organization has developed its information security policies and standards, the information security community can begin developing the blueprint for the information security program. If any policies, standards, or practices have not been completed, management must determine whether to proceed nonetheless with the development of the blueprint. This **information security blueprint** is the basis for the design, selection, and implementation of all security program elements, including policy implementation, ongoing policy management, risk management programs, education and training programs, technological controls, and program maintenance. The security blueprint builds on top of the organization's information security policies. It is a detailed version of the **information security framework**. The blueprint specifies tasks and the order in which they are to be accomplished, just as an architect's blueprint serves as the design template for the construction of a building. The framework is the philosophical framework from which the blueprint is designed, like the style or methodology in which an architect was trained.

The ISO 27000 Series

One of the most widely referenced security models is the Information Technology—Code of Practice for Information Security Management, which was originally published as British Standard BS7799. In 2000, this code of practice was adopted as ISO/IEC 17799, an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The document was revised in 2005 to become ISO 17799:2005, and then it was renamed as ISO 27002 in 2007 to align it with ISO 27001, which is discussed later in this chapter. While the details of ISO/IEC 27002 are available only to those who purchase the standard, its structure and general organization are well known.

NIST Security Models

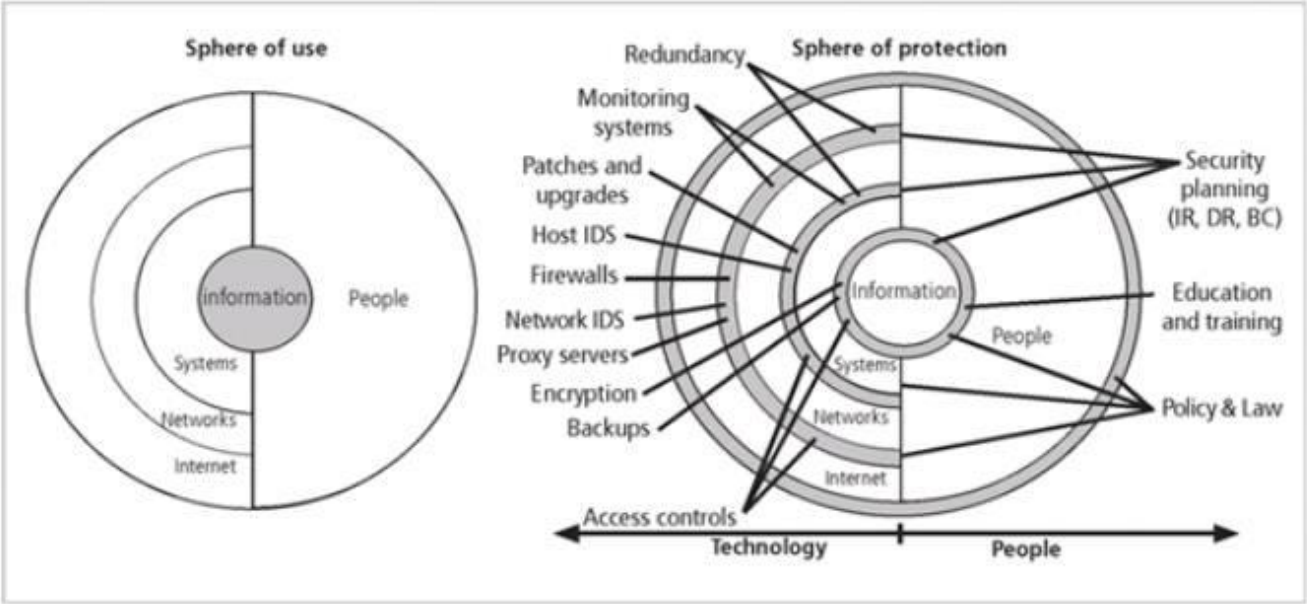
Other approaches are described in the many documents available from the NIST Computer Security Resource Center (http://csrc.nist.gov). Because the NIST documents are publicly available at no charge and have been for some time, they have been broadly reviewed by government and industry professionals and were among the references cited by the U.S. government when it decided not to select the ISO/IEC 17799 standards. The following NIST documents can assist in the design of a security framework:

- SP 800-12: An Introduction to Computer Security: The NIST Handbook. Is an excellent reference and guide for the security manager or administrator in the routine management of information security.
- SP800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems. Provides best practices and security principles that can direct the security team in the development of a security blueprint.
- SP 800-18 Rev. 1: Guide for Developing Security Plans for Federal Information Systems. Used as the foundation for a comprehensive security blueprint and framework.
- SP 800-30 Rev. 1: Guide for Conducting Risk Assessments
- SP 800-37 Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View
- SP 800-50: Building an Information Technology Security Awareness and Training Program
- SP 800-55 Rev. 1: Performance Measurement Guide for Information Security
- SP 800-100: Information Security Handbook: A Guide for Managers

Other Sources of Security Framework

- Security Area Working Group acts as advisory board for protocols and areas developed and promoted by the Internet Society.
- The Federal Agency Security Practices (FASP) site (fasp.nist.gov) is designed to provide best practices for public agencies and is adapted easily to private institutions.

The Information Security Blueprint



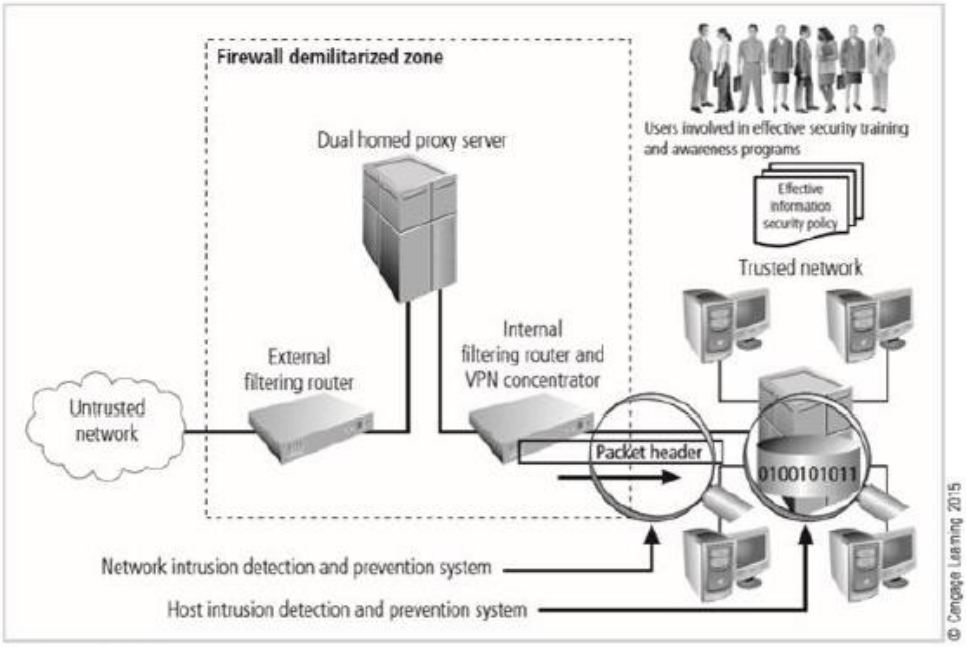
Spheres of Security

The spheres of security, are the foundation of the security framework. Generally speaking, the spheres of security illustrate how information is under attack from a variety of sources. The sphere of use, illustrates the ways in which people access information. For example, people read hard copies of documents and access information through systems. Information, as the most important asset in this model, is at the center of the sphere. Information is always at risk from attacks whenever it is accessible by people or computer systems. Networks and the Internet are indirect threats, as exemplified by the fact that a person attempting to access information from the Internet must traverse local networks.

Levels of Controls

Information security safeguards provide three levels of control: managerial, operational, and technical.

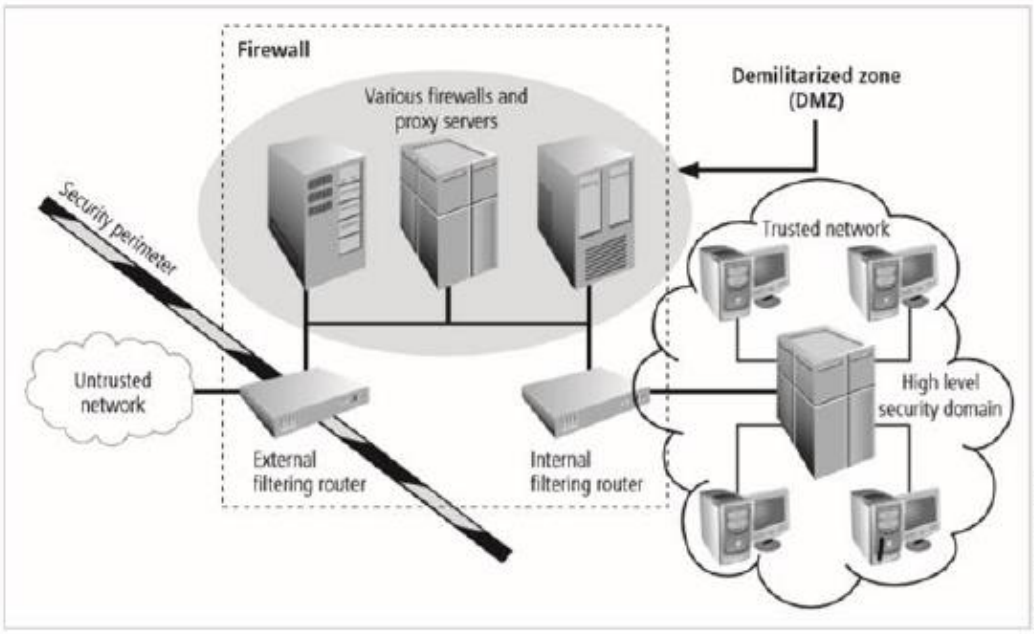
- Managerial controls set the direction and scope of the security process and provide detailed instructions for its conduct.
- Operational controls address personnel security, physical security, and the protection of production inputs and outputs.
- Technical controls are the tactical and technical implementations of security in the organization.



Defense in depth

Defense in Depth

One of the foundations of security architectures is the requirement to implement security in layers. Defense in depth requires that the organization establish sufficient security controls and safeguards, so that an intruder faces multiple layers of controls.



Security perimeters and domains

Security Perimeter

The point at which an organization's security protection ends and the outside world begins is referred to as the security perimeter. Unfortunately, the perimeter does not apply to internal attacks from employee threats or on-site physical threats.

LESSON 3

Security Education, Training, and Awareness Program

Learning Outcomes:

- Explain why organizations implement SETA programs and describe their role in reducing accidental security breaches.
- Differentiate among security education, security training, and security awareness.
- Identify common methods used to raise security awareness.

Understanding Security Education, Training, and Awareness Program

Once your organization has defined the policies that will guide its security program and selected an overall security model by creating or adapting a security framework and a corresponding detailed implementation blueprint, it is time to implement a security education, training, and awareness (SETA) program. The SETA program is the responsibility of the CISO and is a control measure designed to reduce incidents of accidental security breaches by employees. Employee errors are among the top threats to information assets, so it is well worth developing programs to combat this threat. SETA programs are designed to supplement the general education and training programs that many organizations use to educate staff about information security.

The SETA program consists of three elements: security education, security training, and security awareness. An organization may not be able or willing to undertake all three of these elements, and it may outsource elements to local educational institutions. The purpose of SETA is to enhance security by doing the following:

- Improving awareness of the need to protect system resources.
- Developing skills and knowledge so computer users can perform their jobs more securely.
- Building in-depth knowledge as needed to design, implement, or operate security programs for organizations and systems25

	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Exposure
Teaching method	Theoretical instruction • Discussion seminar • Background reading • Hands-on practice	Practical instruction • Lecture • Case study workshop • Posters	Media • Videos • Newsletters
Test measure	Essay (interpret learning)	Problem solving (apply learning)	• True or false • Multiple choice (identify learning)
Impact timeframe	Long term	Intermediate	Short term

Comparative Framework of SETA[26]

Source: NIST SP 800-12.

Security Education

Everyone in an organization needs to be trained and made aware of information security, but not everyone needs a formal degree or certificate in information security. When management agrees that formal education is appropriate, an employee can investigate courses in continuing education from local institutions of higher learning. Several universities have formal coursework in information security.

Security Training

Security training provides employees with detailed information and hands-on instruction to prepare them to perform their duties securely. Management of information security can develop customized inhouse training or outsource the training program.

Security Awareness

A security awareness program is one of the least frequently implemented but most beneficial programs in an organization. A security awareness program is designed to keep information security at the forefront of users' minds. These programs don't have to be complicated or expensive. Good programs can include newsletters, security posters, videos, bulletin boards, flyers, and trinkets. The security newsletter is the most cost-effective method of disseminating security information and news to employees. Newsletters can be distributed via hard copy, e-mail, or intranet.

LESSON 4

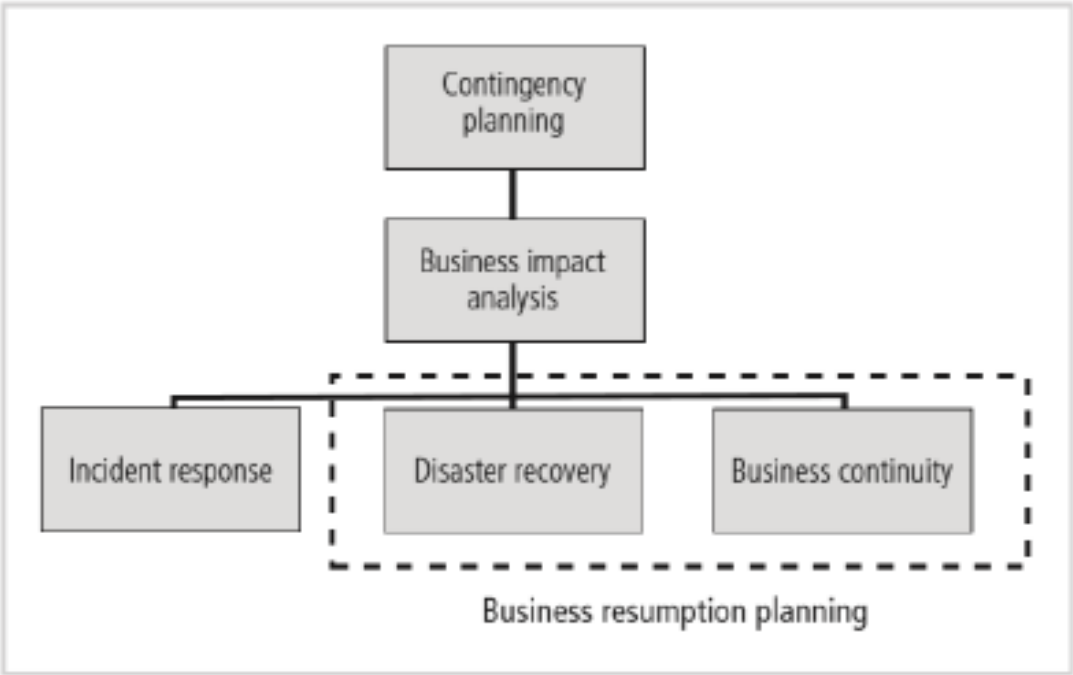
Continuity Strategies

Learning Outcomes:

- Understand contingency planning, its key components (IRP, DRP, BCP), and the roles of the CPMT.
- Explain the Business Impact Analysis (BIA) and the phases of incident response.
- Describe disaster recovery, business continuity actions, crisis management, and when law enforcement involvement is needed.

Understanding Continuity Strategies

A key role for all managers is **contingency planning (CP)**. Managers in the IT and information security communities are usually called on to provide strategic planning to assure the continuous availability of information systems. Unfortunately for managers, however, the probability that some form of attack will occur—from inside or outside, intentional or accidental, human or nonhuman, annoying or catastrophic— is very high. Thus, managers from each community of interest must be ready to act when a successful attack occurs.



Components of contingency planning

A contingency plan is prepared by the organization to anticipate, react to, and recover from events that threaten the security of information and information assets in the organization. This plan also helps restore the organization to normal modes of business operations after an event. The discussion of contingency planning begins by explaining the differences among its various elements and examining the points at which each element is brought into play.

CP includes incident response planning (IRP), disaster recovery planning (DRP), and business continuity planning (BCP), in preparation for adverse events that become incidents or disasters. The primary functions of these three types of planning are as follows:

- The **incident response plan (IR plan)** focuses on immediate response, but if the attack escalates or is disastrous (for example, a fire, flood, earthquake, or total blackout), the process moves on to disaster recovery and the BC plan.
- The **disaster recovery plan (DR plan)** typically focuses on restoring systems at the original site after disasters occur, and so is closely associated with the BC plan.
- The **business continuity plan (BC plan)** occurs concurrently with the DR plan when the damage is major or ongoing, and requires more than simple restoration of information and information resources. The BC plan establishes critical business functions at an alternate site.

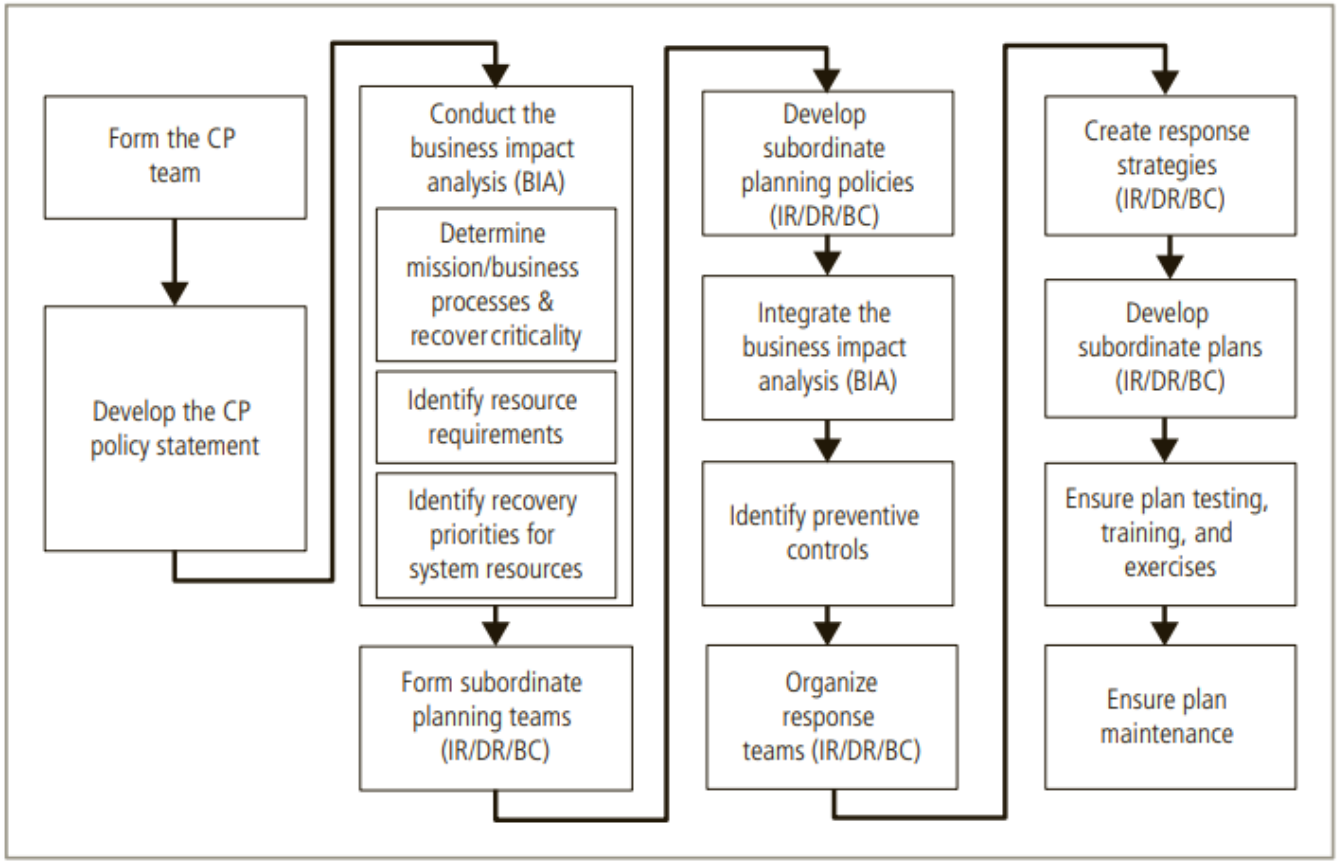


Figure 4-14 Major steps in contingency planning

Contingency Planning Team

Before any planning can begin, a team has to plan the effort and prepare the resulting documents

- **Champion** - A high-level manager to support, promote, and endorse the findings of the project
- **Project Manager** - Leads the project and makes sure a sound project planning process is used, a complete and useful project plan is developed, and project resources are prudently managed
- **Team Members** - Should be the managers or their representatives from the various communities of interest: business, IT, and information security

Business Impact Analysis

The first phase in developing the contingency planning process is the business impact analysis (BIA). The BIA, a preparatory activity common to both CP and risk management, helps determine which business functions and information systems are the most critical to the success of the organization.

According to NIST's SP 800-34, Rev. 1, the CPMT conducts the BIA in three stages:

1. Determine mission/business processes and recovery criticality.
2. Identify recovery priorities for system resources.
3. Identify resource requirements.

Determine Mission/Business Processes and Recovery Criticality

The first major BIA task is the analysis and prioritization of business processes within the organization, based on their relationship to the organization's mission. Each business department, unit, or division must be independently evaluated to determine how important its functions are to the organization as a whole. For example, recovery operations would probably focus on the IT Department and network operation before turning to the Personnel Department's hiring activities. Likewise, recovering a manufacturing company's assembly line is more urgent than recovering its maintenance tracking system. Personnel functions and assembly line maintenance are important, but unless the organization's main revenue-producing operations can be restored quickly, other functions are irrelevant. It is important to collect critical information about each business unit before prioritizing the business units.

Identify Recovery Priorities for System Resources

As the CPMT conducts the BIA, it will assess priorities and relative values for mission/business processes. To do so, it needs to understand the information assets used by those processes. The presence of high value information assets may influence the valuation of a particular business process. Normally, this task would be performed as part of the risk assessment function within the risk management process. The organization should identify, classify, and prioritize its information assets, placing classification labels on each collection or repository of information to better understand its value and prioritize its protection. If the organization has not performed this task, the BIA process is the appropriate time to do so.

Identify Resource Requirements

Once the organization has created a prioritized list of its mission and business processes, it needs to determine which resources would be required to recover those processes and associated assets. Some processes are resource intensive, like IT functions. Supporting customer data, production data, and other organizational information requires extensive quantities of information processing, storage, and transmission (through networking). Other business production processes require complex or expensive components to operate.

Incident Response Planning

Incident response planning includes the identification and classification of an incident and the response to it. The IR plan is made up of activities that must be performed when an incident has been identified. Before developing such a plan, you should understand the philosophical approach to incident response planning. If an action that threatens information occurs and is completed, it is classified as an incident. All of the threats identified in earlier chapters could result in attacks that would be classified as information security incidents. For purposes of this discussion, however, adverse events are classified as incidents if they have the following characteristics:

- They are directed against information assets.
- They have a realistic chance of success.
- They could threaten the confidentiality, integrity, or availability of information resources.

Incident response planning focuses on detecting and correcting the impact of an incident on information assets. Prevention is purposefully omitted, as this activity is more a function of general information security than of incident response. In other words, IR is more reactive than proactive, with the exception of the planning that must occur to prepare IR teams to react to an incident. IR consists of the following four phases:

1. Planning
2. Detection
3. Reaction
4. Recovery

Incident Planning

Planning for an incident requires a detailed understanding of the scenarios developed for the BIA. With this information in hand, the planning team can develop a series of predefined responses that guide the organization's IR team and information security staff. These responses enable the organization to react quickly and effectively to the detected incident. This discussion assumes that the organization has an IR team and that the organization can detect the incident.

Incident Detection

Members of an organization sometimes notify systems administrators, security administrators, or their managers of an unusual occurrence. This occurrence most often causes a complaint to the help desk from one or more users about a technology service. Complaints are often collected by the help desk, and can include reports such as “the system is acting unusual”, “programs are slow”, “my computer is acting weird” or “data is not available.” Incident detection relies on either a human or automated system (often the help desk staff) to identify an unusual occurrence and classify it properly. The mechanisms that might detect an incident include intrusion detection and prevention systems (both host-based and network-based), virus detection software, systems administrators, and even end users. Intrusion detection systems and virus detection software are examined in detail in later chapters. This chapter focuses on the human element.

Incident Reaction

Incident reaction consists of actions outlined in the IR plan that guide the organization in attempting to stop the incident, mitigate its impact, and provide information for recovery. These actions take place as soon as the incident is over. Several actions must occur quickly, including notification of key personnel and documentation of the incident. These actions should be prioritized and documented in the IR plan for quick use in the heat of the moment.

Incident Containment Strategies The first priority of incident reaction is to stop the incident or contain its scope or impact. Unfortunately, the most direct means of containment, sometimes known as “cutting the wire,” is often not an option for an organization. Incident containment strategies vary depending on the incident and on the amount of damage it causes or may cause. Before an incident can be contained, an organization needs to determine which information and information systems have been affected. The organization can stop the incident and attempt to recover control using several strategies. If the incident;

- originates outside the organization, the simplest and most straightforward approach is to sever the affected circuits.
- is using compromised accounts, the accounts can be disabled.
- is coming in through a firewall, the firewall can be reconfigured to block that particular traffic.

- is using a particular service or process, that process or service can be disabled temporarily.
- is using the organization's systems to propagate itself, you can take down that particular application or server.

The ultimate containment option, which is reserved for only the most drastic scenarios, involves a full stop of all computers and network devices in the organization. Obviously, this step is taken only when all control of the infrastructure has been lost, and the only hope is to preserve the data stored on those computers so it can possibly be used in the future to restore operations.

Incident Recovery

Once the incident has been contained and control of the systems is regained, the next stage of the IR plan is incident recovery. This stage of the plan must be executed immediately. As with incident reaction, the first task is to identify needed human resources and launch them into action. Almost simultaneously, the organization must assess the full extent of the damage to determine how to restore the system to a fully functional state. Next, the process of computer forensics determines how the incident occurred and what happened. These facts emerge from a reconstruction of the data recorded before and during the incident. Next, the organization repairs vulnerabilities, addresses any shortcomings in its safeguards, and restores systems data and services.

Damage Assessment

Incident damage assessment is the immediate determination of the scope of the breach of CIA of information and assets after an incident. There are several sources of information on the type, scope, and extent of damage, including system logs, intrusion detection logs, configuration logs and documents, the documentation from the incident response, and the results of a detailed assessment of systems and data storage. Based on this information, the IR team must begin to examine the current state of the information and systems and compare them to a known state. Related to the task of incident damage assessment is the field of computer forensics. Computer forensics is the process of collecting, analyzing, and preserving computer-related evidence. Evidence proves an action or intent. Computer evidence must be carefully collected, documented, and maintained to be acceptable in formal or informal proceedings.

Circumstances requires that individuals who look for the damage receive special training, should it be determined that the incident is part of a crime or may result in a civil action.

Recovery

Once the extent of the damage has been determined, the recovery process can begin in earnest. Full recovery from an incident requires the following actions:

1. Identify the vulnerabilities that allowed the incident to occur and spread. Resolve them.
2. Address the safeguards that failed to stop or limit the incident, or that were missing from the system in the first place. Install, replace, or upgrade these safeguards.
3. Evaluate monitoring capabilities if they are present. Improve their detection and reporting methods or install new monitoring capabilities.
4. Restore the data from backups.
5. Restore the services and processes in use.
6. Continuously monitor the system
7. Restore confidence to the organization's communities of interest.

Disaster Recovery Planning

Disaster recovery (DR) planning is the process of preparing an organization to handle a disaster and recover from it, whether the disaster is natural or man-made. The key emphasis of a DR plan is to reestablish operations at the primary site, the location at which the organization performs its business. The goal of the plan is to make things whole, or as they were before the disaster.

The Disaster Recovery Plan

Similar in structure to the IR plan, the DR plan provides detailed guidance in the event of a disaster. It is organized by the type or nature of the disaster, and it specifies recovery procedures during and after each type of disaster. It also provides details about the roles and responsibilities of the people involved in the DR effort, and it identifies the personnel and agencies that must be notified. The DR plan must be tested using the same testing mechanisms as the IR plan. At a minimum, the DR plan must be reviewed periodically during a walk-through or talk-through.

Recovery Operations

Reactions to a disaster can vary so widely that it is impossible to describe the process with any accuracy. Each organization must examine the scenarios developed at the start of contingency planning and determine how to respond. Should the physical facilities be spared after the disaster, the disaster recovery team should begin restoring systems and data to reestablish full operational capability. If the organization's facilities do not survive, alternative actions must be taken until new facilities can be acquired. When a disaster threatens the viability of the organization at the primary site, the disaster recovery process transitions into the process of business continuity planning.

Business Continuity Planning

Business continuity planning prepares an organization to reestablish or relocate critical business operations during a disaster that affects operations at the primary site. If a disaster has rendered the current location unusable, a plan must be in place to allow the business to continue to function. Not every business needs such a plan or such facilities. Small companies or fiscally sound organizations may have the latitude to cease operations until the physical facilities can be restored. Manufacturing and retail organizations may not have this option because they depend on physical commerce and may not be able to relocate operations.

Developing Continuity Programs

Once the incident response and disaster recovery plans are in place, the organization needs to consider finding temporary facilities to support its continued viability in a disaster. A BC plan is somewhat simpler to develop than an IR plan or DR plan because it consists primarily of selecting a continuity strategy and integrating the off-site data storage and recovery functions into this strategy. Some components of the BC plan, such as an off-site backup service, could already be integral to the organization's normal operations. Other components require special consideration and negotiation.

Crisis Management

The actions taken during and after a disaster are referred to as crisis management. Crisis management differs dramatically from incident response, as it focuses first and foremost on the people involved. The disaster recovery team works closely with the crisis management team. According to Gartner Research, the crisis management team is: responsible for managing the event from an enterprise perspective and covers the following major activities:

- Supporting personnel and their loved ones during the crisis
- Determining the event's impact on normal business operations and, if necessary, making a disaster declaration
- Keeping the public informed about the event and the actions being taken to ensure the recovery of personnel and the enterprise
- Communicating with major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties.

The Consolidated Contingency Plan

Using the strategy described earlier, an organization can build a single document that combines all aspects of the contingency policy and plan, incorporating the IR, DR, and BC plans. In large organizations, such a document may be massive; because it would be unwieldy in physical form, it is often created and stored electronically in a safe and secure off-site location. The document should be online and easily accessible via the Internet by appropriate employees in time of need. The document may be stored in an encrypted file and within a password-protected repository. Small and medium-sized organizations can use the same approach, but they may also store hard copies of the document both within and outside the organization, at the residences of people who may need them.

Law Enforcement Involvement

Sometimes, an attack, breach of policy, or other incident constitutes a violation of law. Perhaps the incident was originally considered an accident but turns out to have been an attempt at corporate espionage, sabotage, or theft. The involvement of law enforcement agencies has advantages and disadvantages. The agencies may be much more capable of processing evidence than an organization.

In fact, unless the organization's security forces have been trained in processing evidence and computer forensics, they may do more harm than good when extracting the necessary information to legally convict a suspected criminal. Law enforcement agencies can issue the warrants and subpoenas necessary to document a case, and are adept at obtaining statements from witnesses, affidavits, and other required documents. Law enforcement personnel can be a security administrator's greatest ally in the war on computer crime. Therefore, organizations should get to know the local and state officials charged with enforcing information security laws before having to make a call to report a suspected crime.

LESSON SUMMARY

Information security governance is the application of the principles of corporate governance to the information security function. These principles include executive management's responsibility to provide strategic direction, ensure the accomplishment of objectives, oversee that risks are appropriately managed, and validate responsible resource use.

Management must use policies as the basis for all information security planning, design, and deployment. Policies direct how issues should be addressed and technologies should be used.

Management has essential role in development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines.

Information security blueprint is planning document that is basis for design, selection, and implementation of all security policies, education and training programs, and technological controls.

Information security policy is best disseminated in a comprehensive security education, training, and awareness (SETA) program. A security awareness program is one of the least frequently implemented but most beneficial programs in an organization. A security awareness program is designed to keep information security at the forefront of users' minds.

Contingency planning (CP) made up of three components: incident response planning (IRP), disaster recovery planning (DRP), and business continuity planning (BCP).

Crisis management refers to the actions an organization takes during and immediately after a disaster. Crisis management focuses first and foremost on the people involved.

KEY TERMS

- Strategic Planning
- Operational Planning
- Tactical Planning
- Strategic Plan
- Operational Plan
- Tactical Plan
- Governance
- Information Security Governance
- Policy
- Guidelines
- Practices
- Procedures
- Standard
- Enterprise Information Security Policy (EISP)
- Issue-specific Security Policy (ISSP)
- Systems-specific Security Policies (SysSPs)
- Access Control List (ACL)
- Information Security Framework
- Defense In Depth
- Security Education, Training, And Awareness (SETA)
- Contingency Planning (CP)
- Business Continuity Plan (BC Plan)
- Business Continuity Planning (BCP)
- Disaster
- Disaster Recovery Plan (DR Plan)
- Disaster Recovery Planning (DRP)
- Incident Response Plan (IR Plan)
- Incident Response Planning (IRP)
- Business Impact Analysis (BIA)

REFERENCES

Electronic Books

- Whiteman, et.al. “Principles of Information Security”, 3rd Edition