COURSE TECHNOLOGY
CENGAGE Learning™

Principles of Information Security, Fifth Edition

Chapter 4

Planning for Security

Begin with the end in mind.

STEPHEN COVEY, AUTHOR OF *SEVEN HABITS OF HIGHLY EFFECTIVE PEOPLE*

Learning Objectives

- Upon completion of this material, you should be able to:
  - Describe management's role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines
  - Explain what an information security blueprint is, identify its major components, and explain how it supports the information security program

Learning Objectives (cont'd)

- Discuss how an organization institutionalizes its policies, standards, and practices using education, training, and awareness programs
- Describe what contingency planning is and how it relates to incident response planning, disaster recovery planning, and business continuity plans

Introduction

- Information security program begins with policies, standards, and practices, which are the foundation for information security architecture and blueprint.
- Coordinated planning is required to create and maintain these elements.
- Strategic planning for the management of allocation of resources
- Contingency planning for the preparation of uncertain business environment

Information Security Planning and Governance

- Planning levels help translate organization's strategic plans into tactical objectives.
- Planning and the CISO
- Information Security Governance
  - Governance:
    - Set of responsibilities and practices exercised by the board and executive management
    - Goal to provide strategic direction, establishment of objectives, and measurement of progress toward objectives
    - Also verifies/validates that risk management practices are appropriate and assets used properly

Information Security Planning and Governance (cont'd)

- Information Security Governance outcomes
  - Five goals:
    - Strategic alignment
    - Risk management
    - Resource management
    - Performance measures
    - Value delivery

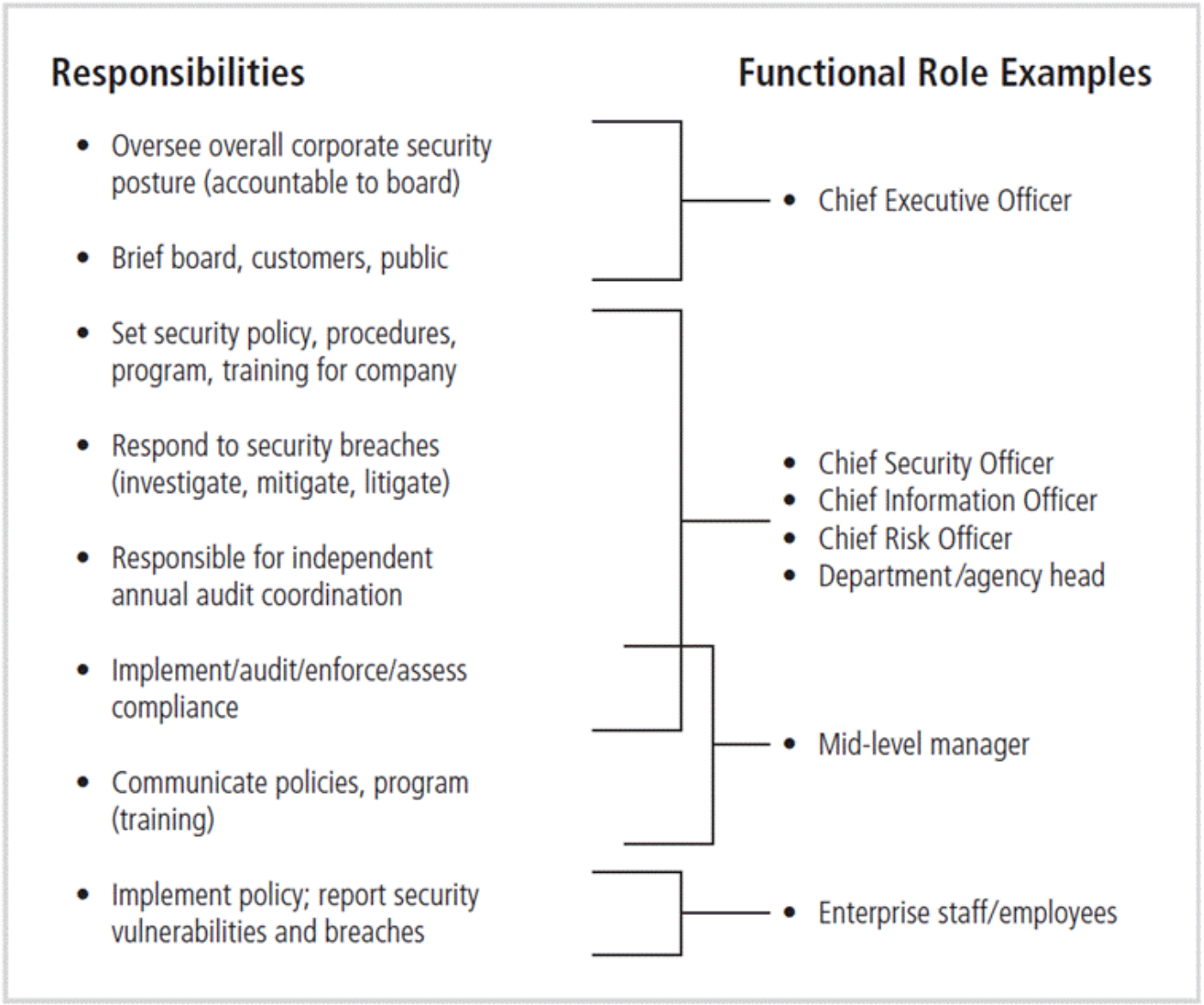

Figure 4-1 Information security governance roles and responsibilities

Information Security Policy, Standards, and Practices

- Management from communities of interest must make policies the basis for all information security planning, design, and deployment.
- Policies direct how issues should be addressed and technologies used.
- Policies should never contradict law, must be able to stand up in court, and must be properly administered.
- Security policies are the least expensive controls to execute but most difficult to implement properly.

Policy as the Foundation for Planning

- Policy functions as organizational law that dictates acceptable and unacceptable behavior.
- Standards: more detailed statements of what must be done to comply with policy
- Practices, procedures, and guidelines effectively explain how to comply with policy.
- For a policy to be effective, it must be properly disseminated, read, understood, and agreed to by all members of the organization, and uniformly enforced.

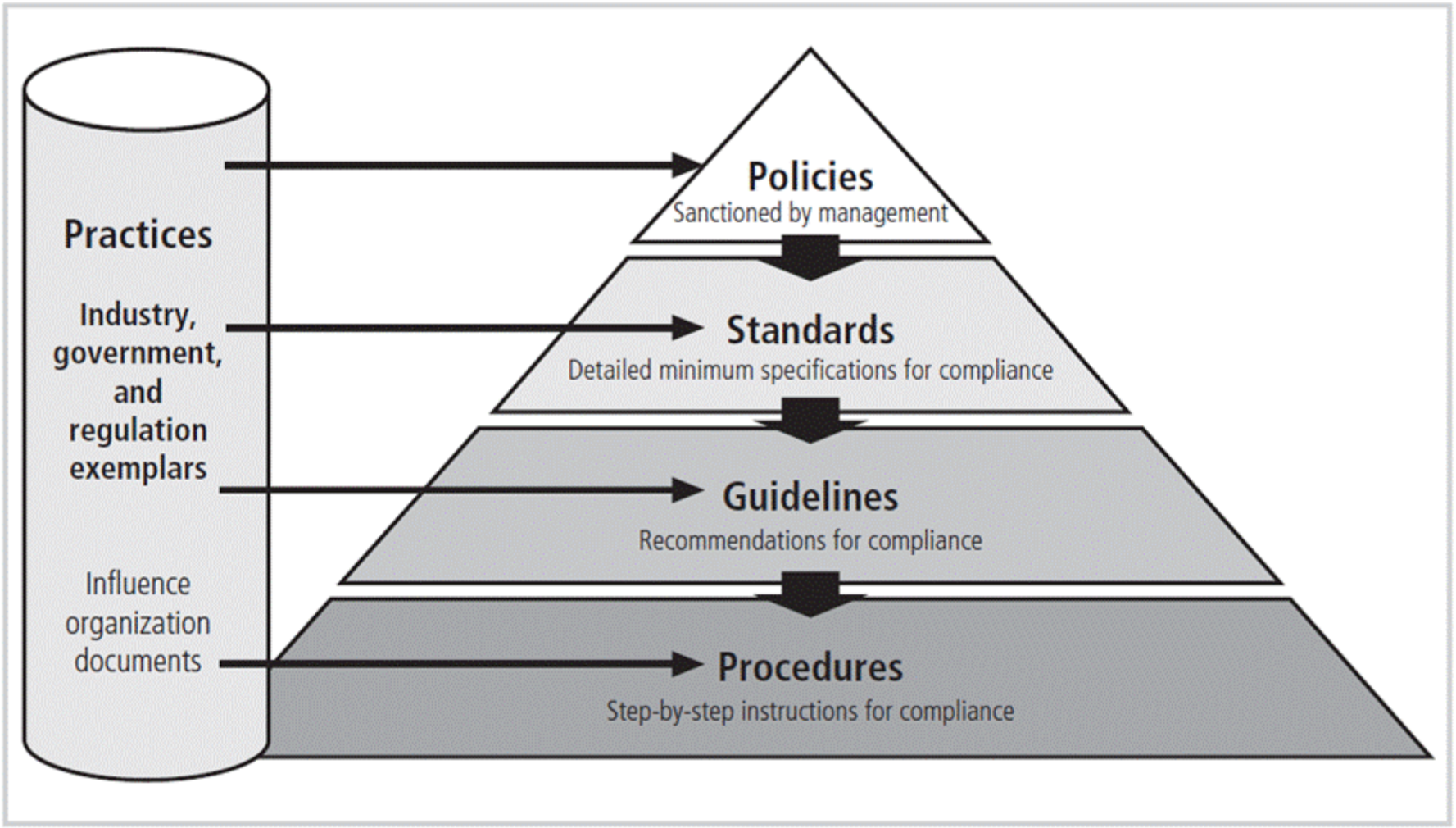

Figure 4-2 Policies, standards, guidelines, and procedures

Enterprise Information Security Policy (EISP)

- Sets strategic direction, scope, and tone for all security efforts within the organization
- Executive-level document, usually drafted by or with Chief Information Officer (CIO) of the organization
- Typically addresses compliance in two areas:
  - Ensure meeting of requirements to establish program and assigning responsibilities therein to various organizational components
  - Use of specified penalties and disciplinary action

Enterprise Information Security Policy (EISP) (cont'd)

- EISP Elements should include:
  - Overview of corporate security philosophy
  - Information on the structure of the organization and people in information security roles
  - Articulated responsibilities for security shared by all members of the organization
  - Articulated responsibilities for security unique to each role in the organization

Component	Description
Statement of Purpose	Answers the question "What is this policy for?" Provides a framework that helps the reader understand the intent of the document. Can include text such as the following: "This document will: • Identify the elements of a good security policy • Explain the need for information security • Specify the various categories of information security • Identify the information security responsibilities and roles • Identify appropriate levels of security through standards and guidelines This document establishes an overarching security policy and direction for our company. Individual departments are expected to establish standards, guidelines, and operating procedures that adhere to and reference this policy while addressing their specific and individual needs."[8]
Information Security Elements	Defines information security. For example: "Protecting the confidentiality, integrity, and availability of information while in processing, transmission, and storage, through the use of policy, education and training, and technology ..." This section can also lay out security definitions or philosophies to clarify the policy.
Need for Information Security	Provides information on the importance of information security in the organization and the legal and ethical obligation to protect critical information about customers, employees, and markets.
Information Security Responsibilities and Roles	Defines the organizational structure designed to support information security within the organization. Identifies categories of people with responsibility for information security (IT department, management, users) and those responsibilities, including maintenance of this document.
Reference to Other Information Standards and Guidelines	Lists other standards that influence this policy document and are influenced by it, perhaps including relevant federal laws, state laws, and other policies.

Table 4-1 Components of the EISP[9]

Source: Whitman, Townsend, and Aalberts, Communications of the ACM.

Issue-Specific Security Policy (ISSP)

- The ISSP:
  - Addresses specific areas of technology
  - Requires frequent updates
  - Contains statement on the organization's position on specific issue
- Three common approaches when creating and managing ISSPs:
  - Create a number of independent ISSP documents
  - Create a single comprehensive ISSP document
  - Create a modular ISSP document

Issue-Specific Security Policy (ISSP) (cont'd)

- Components of the policy:
  - Statement of policy
  - Authorized access and usage of equipment
  - Prohibited use of equipment
  - Systems management
  - Violations of policy
  - Policy review and modification
  - Limitations of liability

Components of an ISSP
1. Statement of policy a. Scope and applicability b. Definition of technology addressed c. Responsibilities
2. Authorized access and usage of equipment a. User access b. Fair and responsible use c. Protection of privacy
3. Prohibited use of equipment a. Disruptive use or misuse b. Criminal use c. Offensive or harassing materials d. Copyrighted, licensed, or other intellectual property e. Other restrictions
4. Systems management a. Management of stored materials b. Employee monitoring c. Virus protection d. Physical security e. Encryption
5. Violations of policy a. Procedures for reporting violations b. Penalties for violations
6. Policy review and modification a. Scheduled review of policy procedures for modification b. Legal disclaimers
7. Limitations of liability a. Statements of liability b. Other disclaimers as needed

Table 4-2 Components of an ISSP[11]

Systems-Specific Policy (SysSP)

- SysSPs often function as standards or procedures used when configuring or maintaining systems.
- Systems-specific policies fall into two groups:
  - Managerial guidance
  - Technical specifications
- Access control lists (ACLs) can restrict access for a particular user, computer, time, duration—even a particular file.
- Configuration rule policies govern how security system reacts to received data.
- Combination SysSPs combine managerial guidance and technical specifications.

Policy Management

- Policies must be managed as they constantly change.
- To remain viable, security policies must have:
  - A responsible manager
  - A schedule of reviews
  - A method for making recommendations for reviews
  - A policy issuance and revision date
  - Automated policy management

The Information Security Blueprint

- Basis for design, selection, and implementation of all security policies, education and training programs, and technological controls
- Detailed version of security framework (outline of overall information security strategy for organization)
- Specifies tasks and order in which they are to be accomplished
- Should also serve as a scalable, upgradeable, and comprehensive plan for the current and future information security needs

The ISO 27000 Series

- One of the most widely referenced security models
- Standard framework for information security that states organizational security policy is needed to provide management direction and support
- Purpose is to give recommendations for information security management
- Provides a starting point for developing organizational security

ISO 27000 Series Standard	Title or topic	Comment
27000:2014	Series Overview and Terminology	Defines terminology and vocabulary for the standard series
27001:2013	Information Security Management System Specification	Drawn from BS7799:2
27002:2013	Code of Practice for Information Security Management	Renamed from ISO/IEC 17799; drawn from BS7799:1
27003:2010	Information Security Management Systems Implementation Guidelines	Guidelines for project planning requirements for implementing an ISMS
27004:2009	Information Security Measurements and Metrics	Performance measure and metrics for information security management decisions
27005:2011	ISMS Risk Management	Supports 27001, but doesn't recommend any specific risk method
27006:2011	Requirements for Bodies Providing Audit and Certification of an ISMS	Largely intended to support the accreditation of certification bodies providing ISMS certification
27007:2011	Guideline for ISMS Auditing	Focuses on management systems
27008:2011	Guideline for Information Security Auditing	Focuses on security controls
27013:2012	Guideline on the Integrated Implementation of ISO/IEC 20000-1 and ISO/IEC 27001	Support for implementing an integrated dual management system
27014:2013	Information Security Governance Framework	ISO's approach to security governance—guidance on evaluating, directing, monitoring, and communicating information security
27015:2012	Information Security Management Guidelines for Financial Services	Guidance for financial services organizations
27019:2013	Information security management guidelines for process control systems specific to the energy industry	Focused on helping organizations in the energy industry implement ISO standards
Planned 27000 Series Standards		
27009 (DRAFT) (forthcoming)	Industry Sector-Specific Applications of ISO/IEC 27001	
27016 (DRAFT) (forthcoming)	Information security management—Organizational economics	
27017 (DRAFT) (forthcoming)	Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002	
27018 (DRAFT) (forthcoming)	Code of practice for PII protection in public clouds acting as PII processors	

Table 4-4 ISO 27000 Series Current and Planned Standards[17]

Note: Additional 27000 series documents are in preparation and are not included here.

Source: www.iso27001security.com/html/iso27000.html.

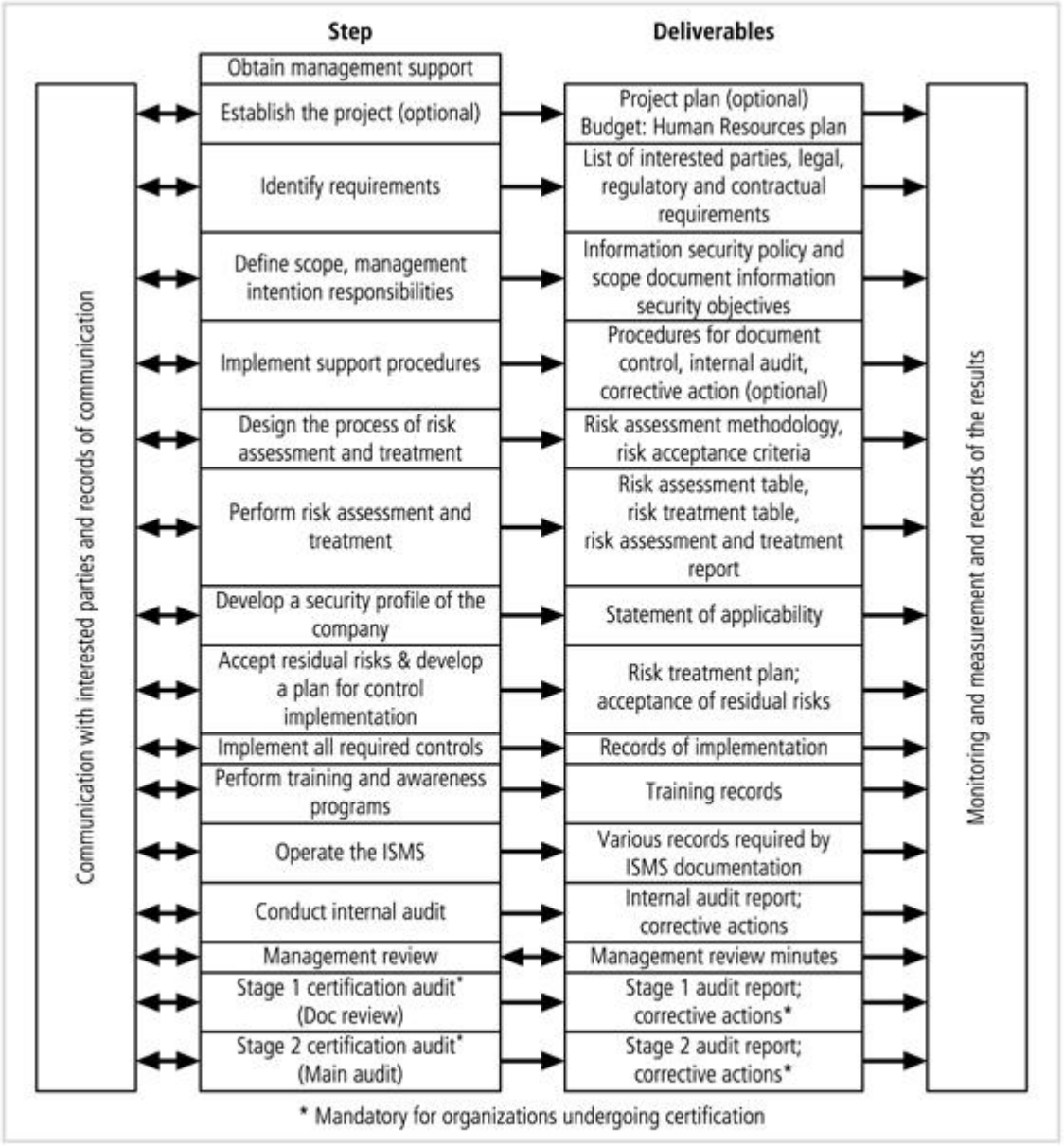

Figure 4-7 ISO/IEC 27001:2013 major process steps

Source: 27001 Academy: ISO 27001 and ISO 22301 Online Consultation Center[16]

NIST Security Models

- Another possible approach described in the documents available from Computer Security Resource Center of NIST
  - SP 800-12
  - SP 800-14
  - SP 800-18 Rev. 1
  - SP 800-26
  - SP 800-30

NIST Special Publication 800-14

- Security supports the mission of the organization and is an integral element of sound management.
- Security should be cost effective; owners have security responsibilities outside their own organizations.
- Security responsibilities and accountability should be made explicit; security requires a comprehensive and integrated approach.
- Security should be periodically reassessed; security is constrained by societal factors.
- Thirty-three principles for securing systems (see Table 4-5)

NIST Cybersecurity Framework

- Consists of three fundamental components:
  - Framework core: set of information security activities an organization is expected to perform and their desired results
  - Framework tiers: help relate the maturity of security programs and implement corresponding measures and functions
  - Framework profile: used to perform a gap analysis between the current and a desired state of information security/risk management

NIST Cybersecurity Framework (cont'd)

- Seven-step approach to implementing/improving programs:
  - Prioritize and scope
  - Orient
  - Create current profile
  - Conduct risk assessment
  - Create target profile
  - Determine, analyze, prioritize gaps
  - Implement action plan

Other Sources of Security Frameworks

- Federal Agency Security Practices (FASP)
- Computer Emergency Response Team Coordination Center (CERT/CC)
- International Association of Professional Security Consultants

Design of Security Architecture

- Spheres of security: foundation of the security framework
- Levels of controls:
  - Management controls set the direction and scope of the security processes and provide detailed instructions for its conduct.
  - Operational controls address personnel and physical security, and the protection of production inputs/outputs.
  - Technical controls are the tactical and technical implementations related to designing and integrating security in the organization.

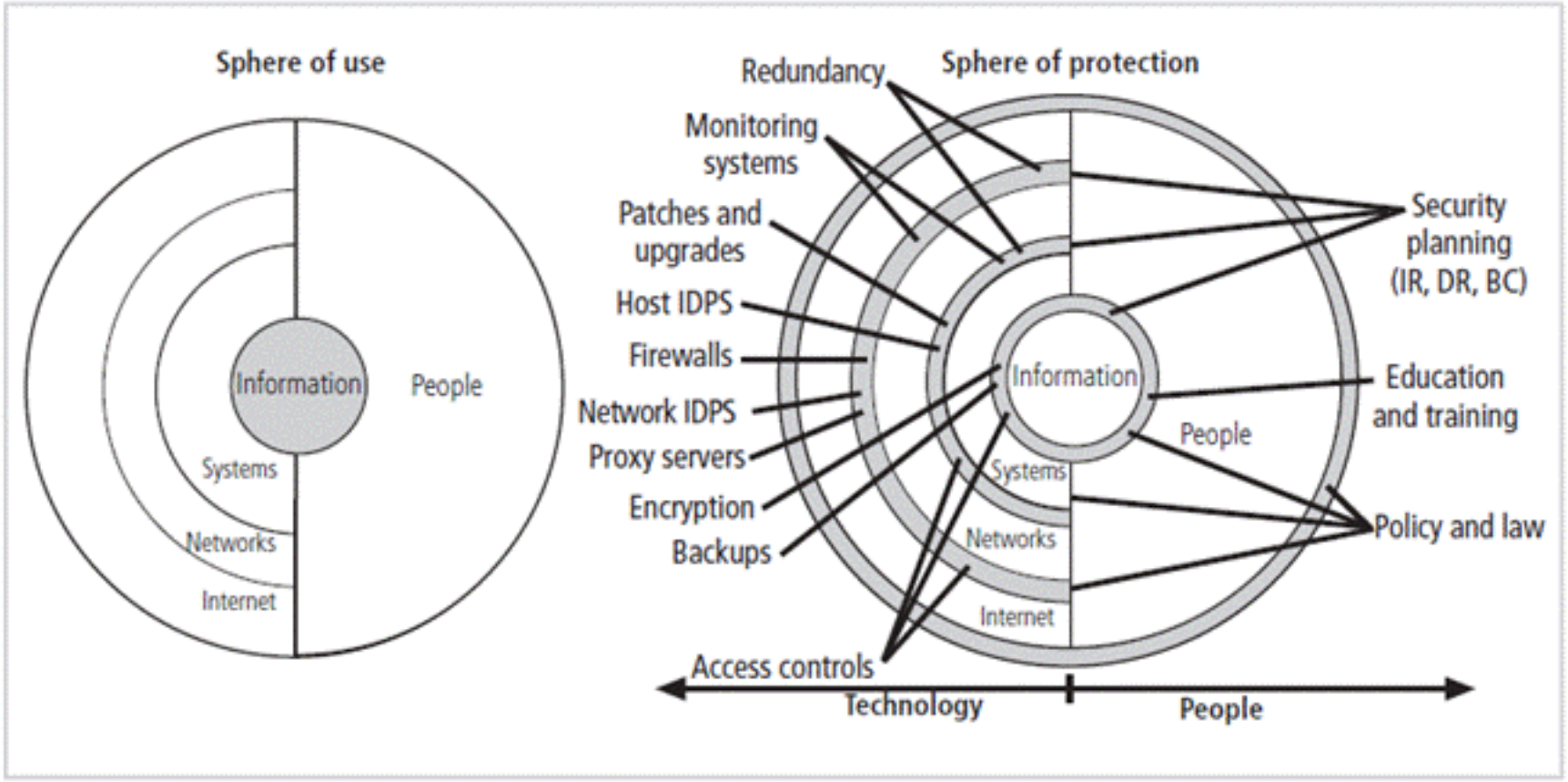

Figure 4-8 Spheres of security

Design of Security Architecture (cont'd)

- Defense in depth
  - Implementation of security in layers
  - Requires that organization establish multiple layers of security controls and safeguards
- Security perimeter
  - Border of security protecting internal systems from outside threats
  - Does not protect against internal attacks from employee threats or onsite physical threats

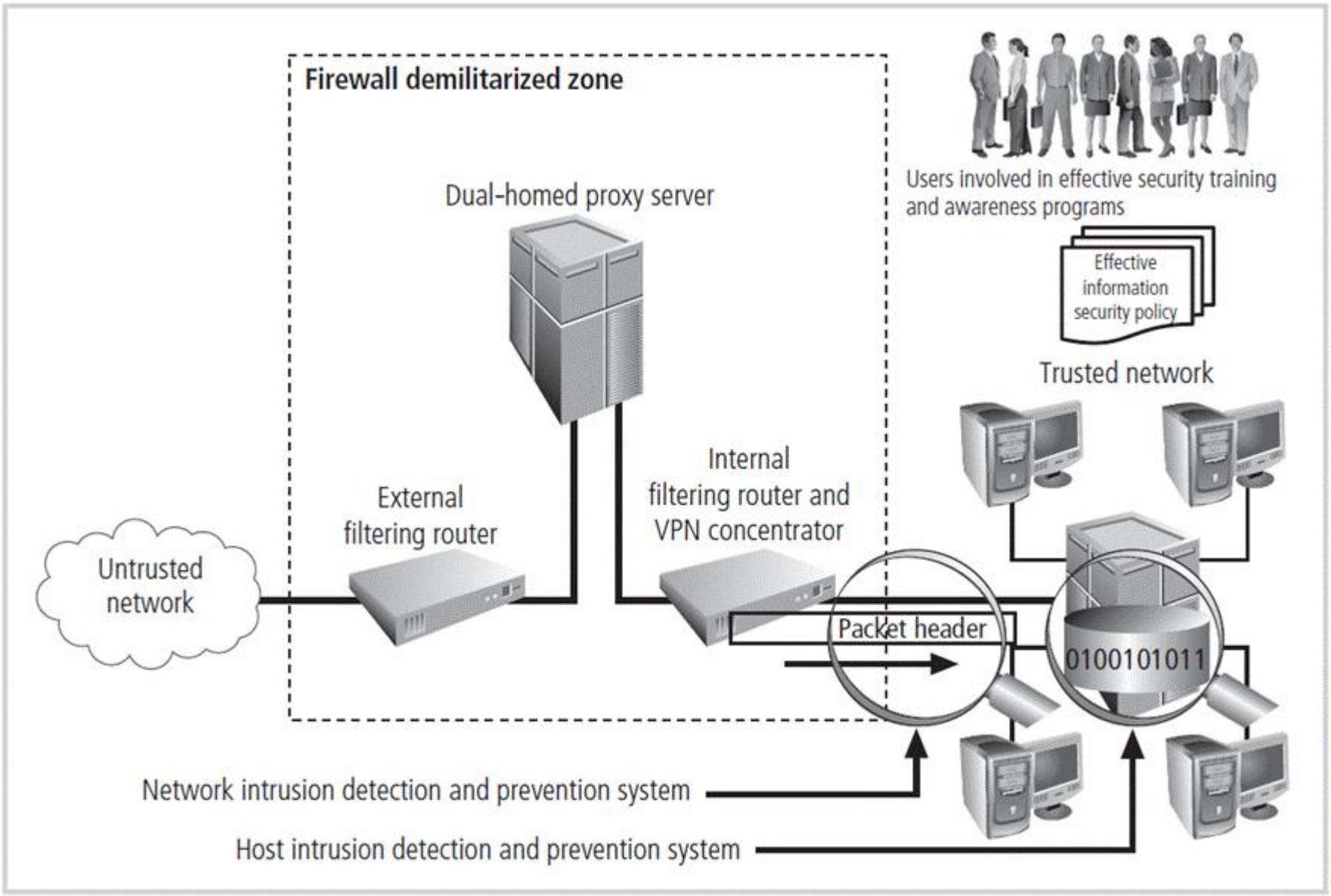

Figure 4-9 Defense in depth

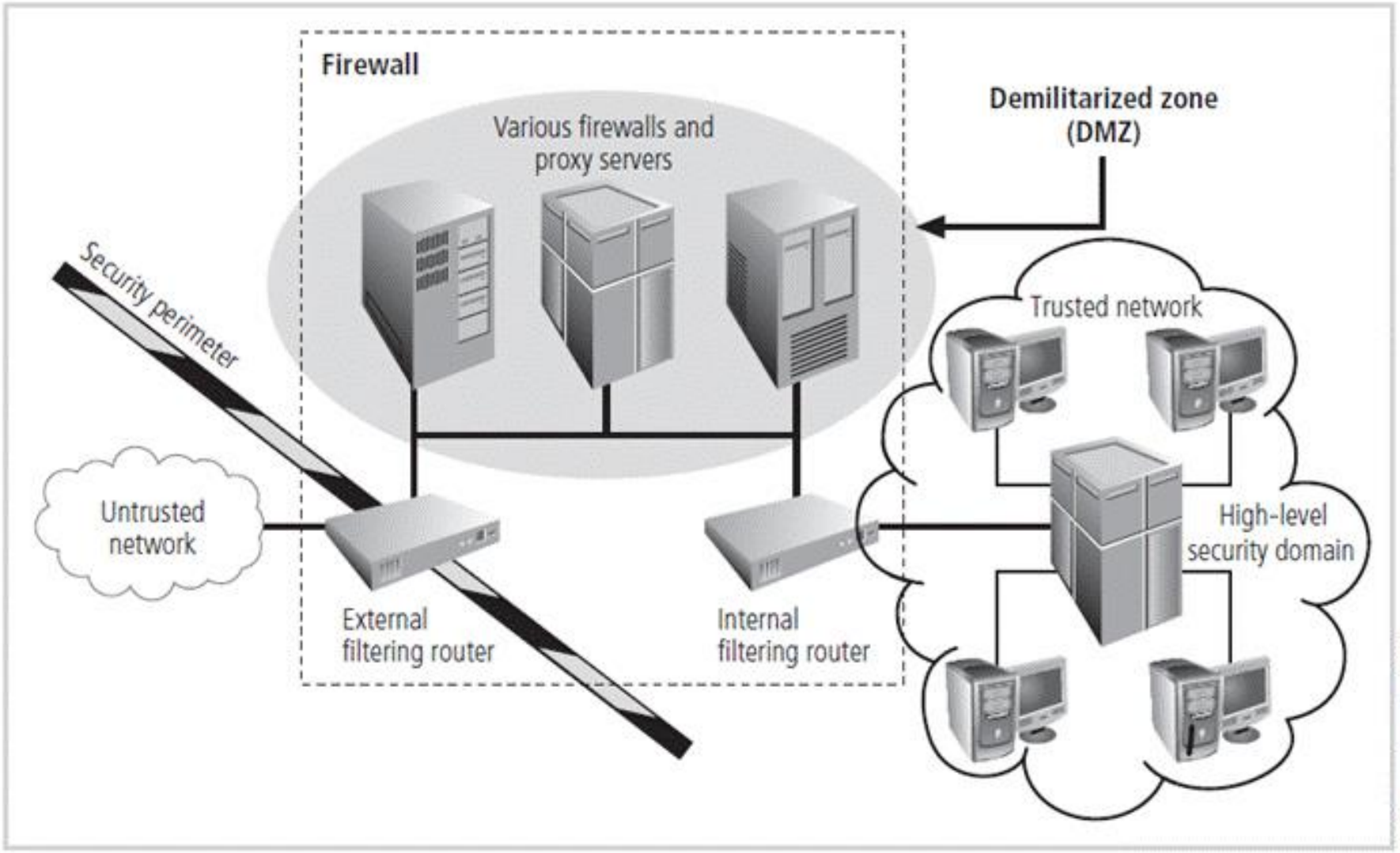

Figure 4-10 Security perimeters and domains

Security Education, Training, and Awareness Program

- Once general security policy exists, implement security education, training, and awareness (SETA) program
- SETA is a control measure designed to reduce accidental security breaches.
- The SETA program consists of security education, security training, and security awareness.
- Enhances security by improving awareness, developing skills, and knowledge, and building in-depth knowledge

Security Education

- Everyone in an organization needs to be trained and aware of information security; not every member needs a formal degree or certificate in information security.
- When formal education is deemed appropriate, an employee can investigate courses in continuing education from local institutions of higher learning.
- A number of universities have formal coursework in information security.

Security Training

- Provides members of the organization with detailed information and hands-on instruction to prepare them to perform their duties securely
- Management of information security can develop customized in-house training or outsource the training program.
- Alternatives to formal training include conferences and programs offered through professional organizations.

Security Awareness

- One of the least frequently implemented but most beneficial programs is the security awareness program.
- Designed to keep information security at the forefront of users' minds
- Need not be complicated or expensive
- If the program is not actively implemented, employees may begin to neglect security matters, and risk of employee accidents and failures are likely to increase.

	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 time frame	Long term	Intermediate	Short term

Table 4-6 Comparative Framework of SETA[26]

Source: NIST SP 800-12.

Continuity Strategies

- Incident response plans (IRPs); disaster recovery plans (DRPs); business continuity plans (BCPs)
- Primary functions of above plans:
  - IRP focuses on immediate response; if attack escalates or is disastrous, process changes to disaster recovery and BCP.
  - DRP typically focuses on restoring systems after disasters occur; as such, it is closely associated with BCP.
  - BCP occurs concurrently with DRP when damage is major or ongoing, requiring more than simple restoration of information and information resources.

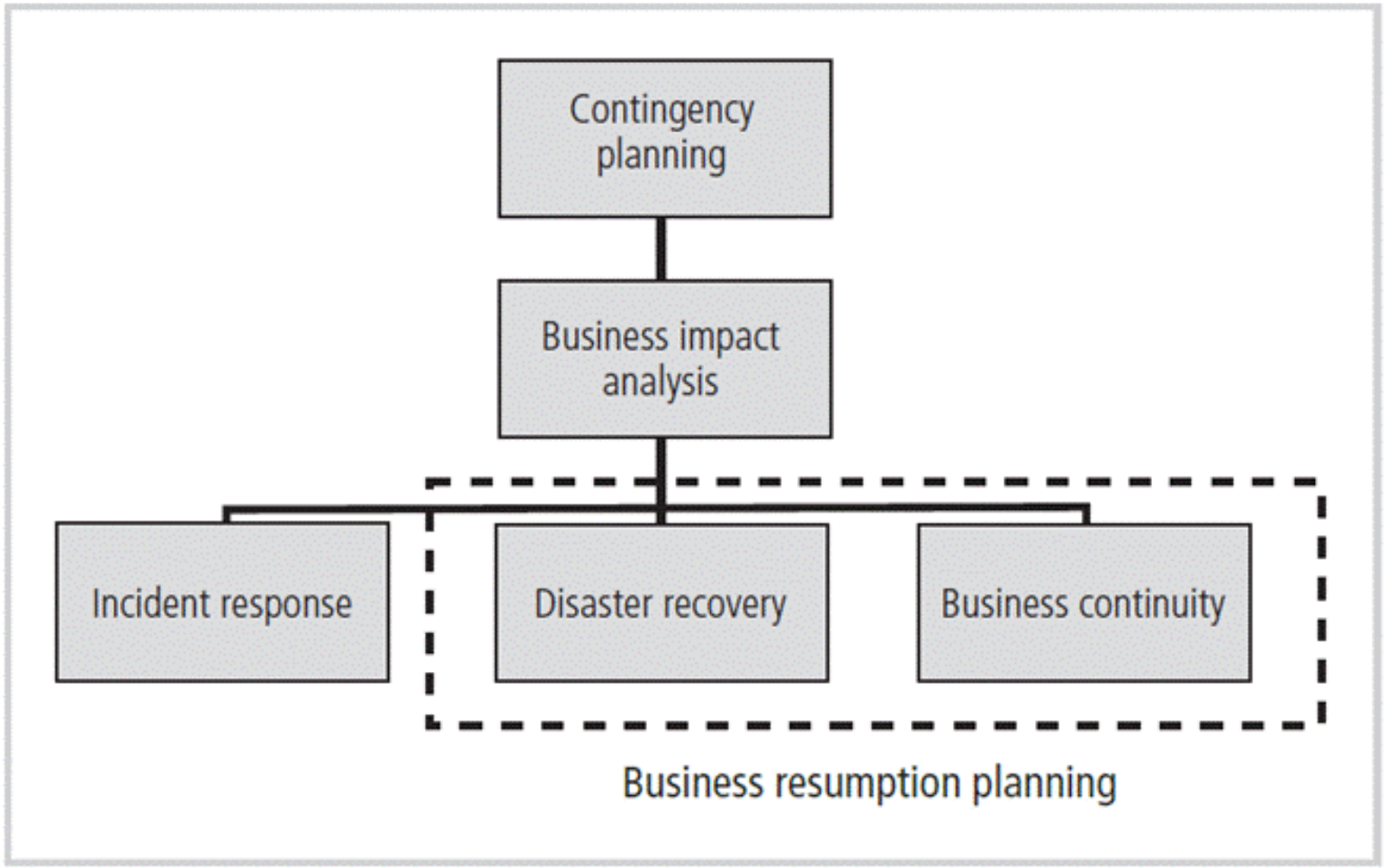

Figure 4-12 Components of contingency planning

Continuity Strategies (cont'd)

- Before planning can actually begin, a team has to start the process.
- Champion: high-level manager to support, promote, and endorse findings of the project
- Project manager: leads project and ensures sound project planning process is used, a complete and useful project plan is developed, and project resources are prudently managed
- Team members: should be managers, or their representatives, from various communities of interest: business, IT, and information security

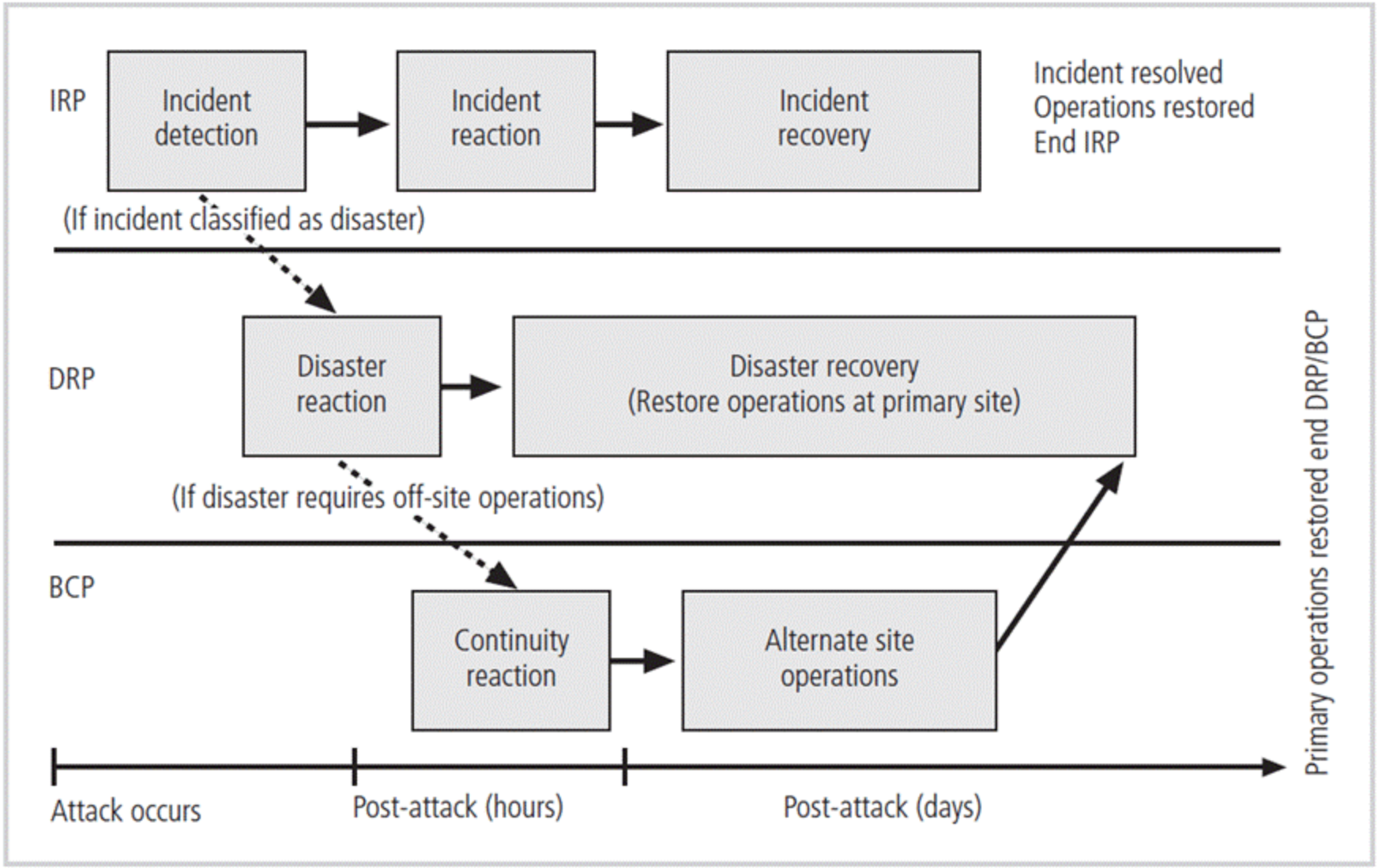

Figure 4-13 Contingency planning timeline

Contingency Planning (CP) Process

- Includes the following steps:
  - Develop CP policy statement
  - Conduct business impact analysis
  - Identify preventive controls
  - Create contingency strategies
  - Develop contingency plan
  - Ensure plan testing, training, and exercises
  - Ensure plan maintenance

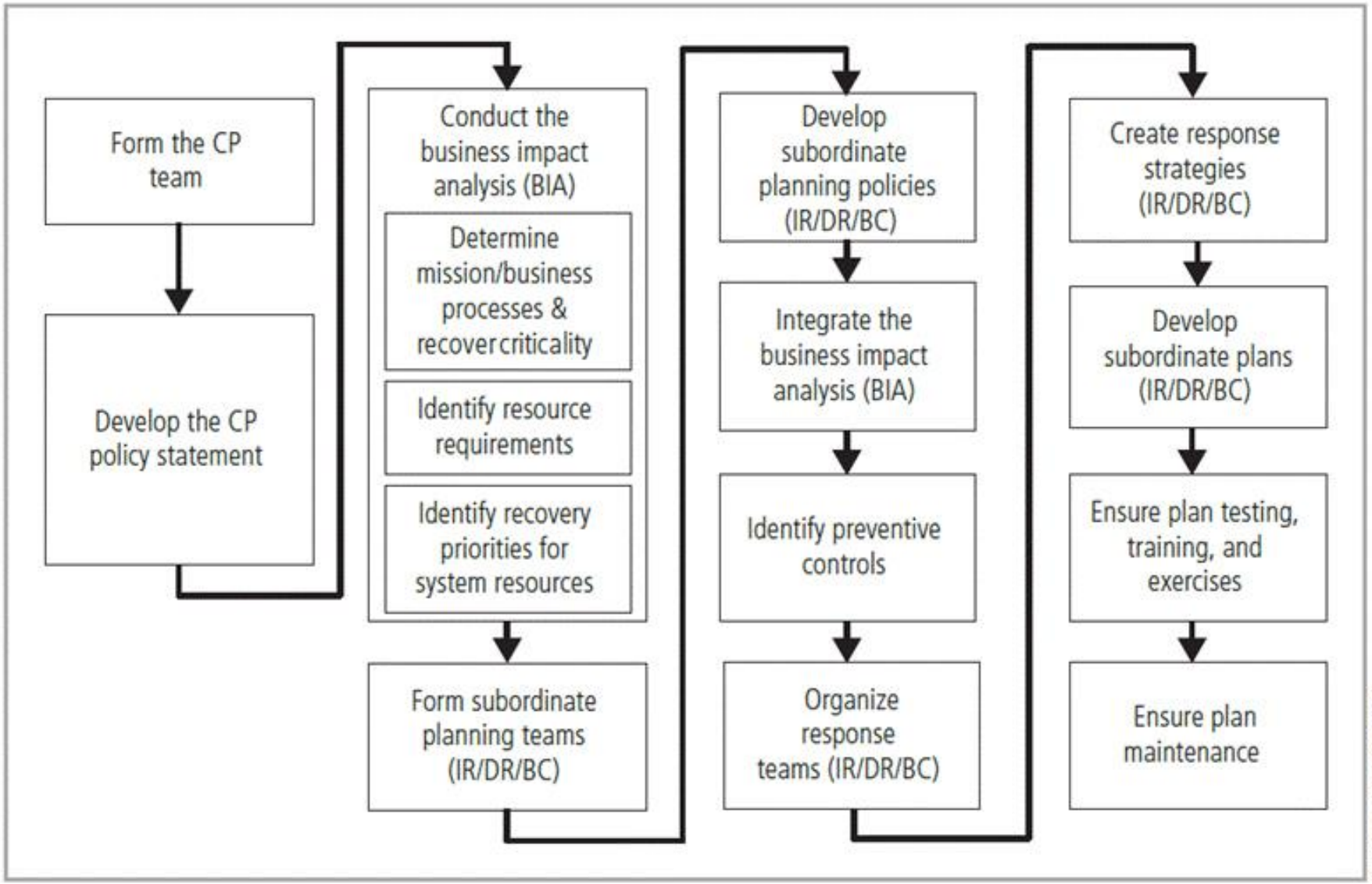

Figure 4-14 Major steps in contingency planning

CP Policy

- Should contain the following sections:
  - Introductory statement of philosophical perspective
  - Statement of scope/purpose
  - Call for periodic risk assessment/BIA
  - Specification of CP's major components
  - Call for/guidance in the selection of recovery options
  - Requirement to test the various plans regularly
  - Identification of key regulations and standards
  - Identification of key people responsible for CP operations
  - Challenge to the organization members for support
  - Administrative information

Business Impact Analysis (BIA)

- Investigation and assessment of various adverse events that can affect organization
- Assumes security controls have been bypassed, have failed, or have proven ineffective, and attack has succeeded
- Organization should consider scope, plan, balance, knowledge of objectives, and follow-ups
- Three stages:
  - Determine mission/business processes and recovery criticality
  - Identify recovery priorities for system resources
  - Identify resource requirements

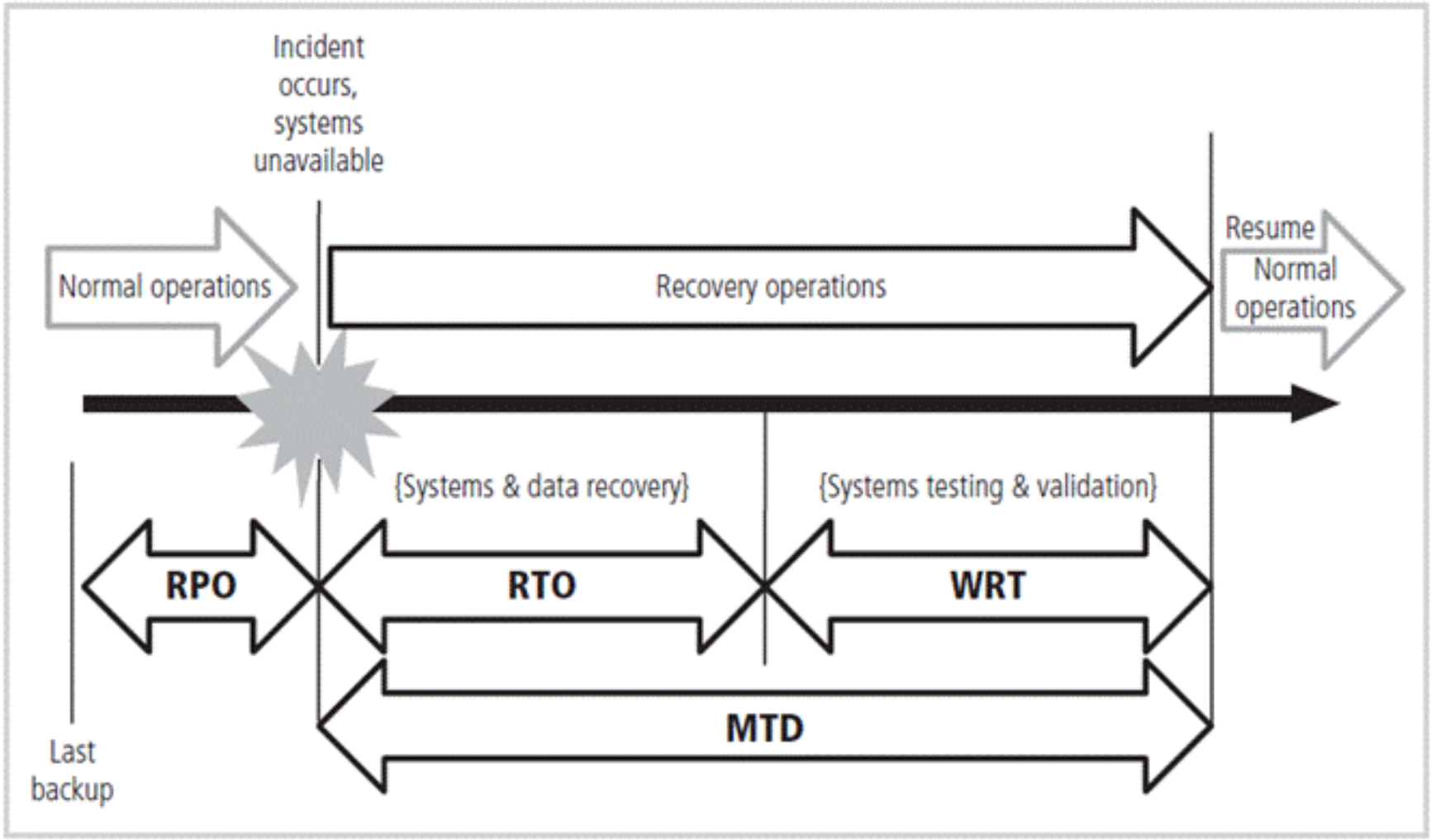

Figure 4-15 RPO, RTO, WRT, and MTD

Incident Response Planning

- Incident response planning includes identification of, classification of, and response to an incident.
- Attacks classified as incidents if they:
  - Are directed against information assets
  - Have a realistic chance of success
  - Could threaten confidentiality, integrity, or availability of information resources
- Incident response (IR) is more reactive than proactive, with the exception of planning that must occur to prepare IR teams to be ready to react to an incident.

Incident Response Planning (cont'd)

- Incident response policy identifies the following key components:
  - Statement of management commitment
  - Purpose/objectives of policy
  - Scope of policy
  - Definition of InfoSec incidents and related terms
  - Organizational structure
  - Prioritization or severity ratings of incidents
  - Performance measures
  - Reporting and contact forms

Incident Response Planning (cont'd)

- Incident Planning
  - Predefined responses enable the organization to react quickly and effectively to the detected incident if:
    - The organization has an IR team
    - The organization can detect the incident
  - IR team consists of individuals needed to handle systems as incident takes place.
- Incident response plan
  - Format and content
  - Storage
  - Testing

Incident Response Planning (cont'd)

- Incident detection
  - Most common occurrence is complaint about technology support, often delivered to help desk.
  - Careful training is needed to quickly identify and classify an incident.
  - Once incident is properly identified, the organization can respond.
  - Incident indicators vary.

Incident Response Planning (cont'd)

- Incident reaction
  - Consists of actions that guide the organization to stop incident, mitigate its impact, and provide information for recovery
  - Actions that must occur quickly:
    - Notification of key personnel
    - Documentation of the incident
- Incident containment strategies
  - Containment of incident's scope or impact as first priority; must then determine which information systems are affected
  - Organization can stop incident and attempt to recover control through a number or strategies.

Incident Response Planning (cont'd)

- Incident recovery
  - Once incident has been contained and control of systems regained, the next stage is recovery.
  - The first task is to identify human resources needed and launch them into action.
  - Full extent of the damage must be assessed.
  - Organization repairs vulnerabilities, addresses any shortcomings in safeguards, and restores data and services of the systems.

Incident Response Planning (cont'd)

- Damage assessment
  - Several sources of information on damage can be used, including system logs, intrusion detection logs, configuration logs and documents, documentation from incident response, and results of detailed assessment of systems and data storage.
  - Computer evidence must be carefully collected, documented, and maintained to be usable in formal or informal proceedings.
  - Individuals who assess damage need special training.

Incident Response Planning (cont'd)

- Automated response
  - New systems can respond to incident threat autonomously.
  - Downsides of current automated response systems may outweigh benefits.
    - Legal liabilities of a counterattack
    - Ethical issues

Disaster Recovery Planning

- Disaster recovery planning (DRP) is preparation for and recovery from a disaster.
- The contingency planning team must decide which actions constitute disasters and which constitute incidents.
- When situations are classified as disasters, plans change as to how to respond; take action to secure most valuable assets to preserve value for the longer term.
- DRP strives to reestablish operations at the primary site.

Business Continuity Planning

- Prepares the organization to reestablish or relocate critical business operations during a disaster that affects operations at the primary site
- If disaster has rendered the current location unusable, there must be a plan to allow business to continue functioning.
- Development of BCP is somewhat simpler than IRP or DRP.
  - Consists primarily of selecting a continuity strategy and integrating off-site data storage and recovery functions into this strategy

Business Continuity Planning (cont'd)

- Continuity strategies
  - There are a number of strategies for planning for business continuity.
  - Determining factor in selecting between options is usually cost.
  - In general, there are three exclusive options: hot sites, warm sites, and cold sites.
  - Three shared functions: time-share, service bureaus, and mutual agreements

Business Continuity Planning (cont'd)

- Off-site disaster data storage
  - To get sites up and running quickly, an organization must have the ability to move data into new site's systems.
  - Options for getting operations up and running include:
    - Electronic vaulting
    - Remote journaling
    - Database shadowing

Crisis Management

- Actions taken in response to an emergency to minimize injury/loss of life, preserve organization's image/market share, and complement disaster recovery/business continuity processes
- What may truly distinguish an incident from a disaster are the actions of the response teams.
- Disaster recovery personnel must know their roles without any supporting documentation.
  - Preparation
  - Training
  - Rehearsal

Crisis Management (cont'd)

- Crisis management team is responsible for managing the event from an enterprise perspective and covers:
  - Supporting personnel and families during crisis
  - Determining impact on normal business operations and, if necessary, making disaster declaration
  - Keeping the public informed
  - Communicating with major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties

Crisis Management (cont'd)

- Key areas of crisis management also include:
  - Verifying personnel head count
  - Checking alert roster
  - Checking emergency information cards

The Consolidated Contingency Plan

- Single document set approach combines all aspects of contingency policy and plan, incorporating IR, DR, and BC plans.
- Often created and stored electronically, it should be easily accessible by employees in time of need.
  - Small- and medium-sized organizations may also store hard copies of the document.

Law Enforcement Involvement

- When incident at hand constitutes a violation of law, the organization may determine involving law enforcement is necessary.
- Questions:
  - When should law enforcement get involved?
  - What level of law enforcement agency should be involved (local, state, federal)?
  - What happens when law enforcement agency is involved?
- Some questions are best answered by the legal department.

Benefits and Drawbacks of Law Enforcement Involvement

- Involving law enforcement agencies has advantages:
  - Agencies may be better equipped at processing evidence.
  - Organization may be less effective in extracting necessary information to legally convict suspected criminal.
  - Law enforcement agencies are prepared to handle any necessary warrants and subpoenas.
  - Law enforcement is skilled at obtaining witness statements and other information collection.

Benefits and Drawbacks of Law Enforcement Involvement (cont'd)

- Involving law enforcement agencies has disadvantages:
  - Once a law enforcement agency takes over the case, the organization cannot control the chain of events.
  - The organization may not hear about the case for weeks or months.
  - Equipment vital to the organization's business may be tagged as evidence.
  - If the organization detects a criminal act, it is legally obligated to involve appropriate law enforcement officials.

Summary

- Management has an essential role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines.
- Information security blueprint is planning the document that is the basis for design, selection, and implementation of all security policies, education and training programs, and technological controls.

Summary (cont'd)

- Information security education, training, and awareness (SETA) is a control measure that reduces accidental security breaches and increases organizational resistance to many other forms of attack.
- Contingency planning (CP) is made up of three components: incident response planning (IRP), disaster recovery planning (DRP), and business continuity planning (BCP).