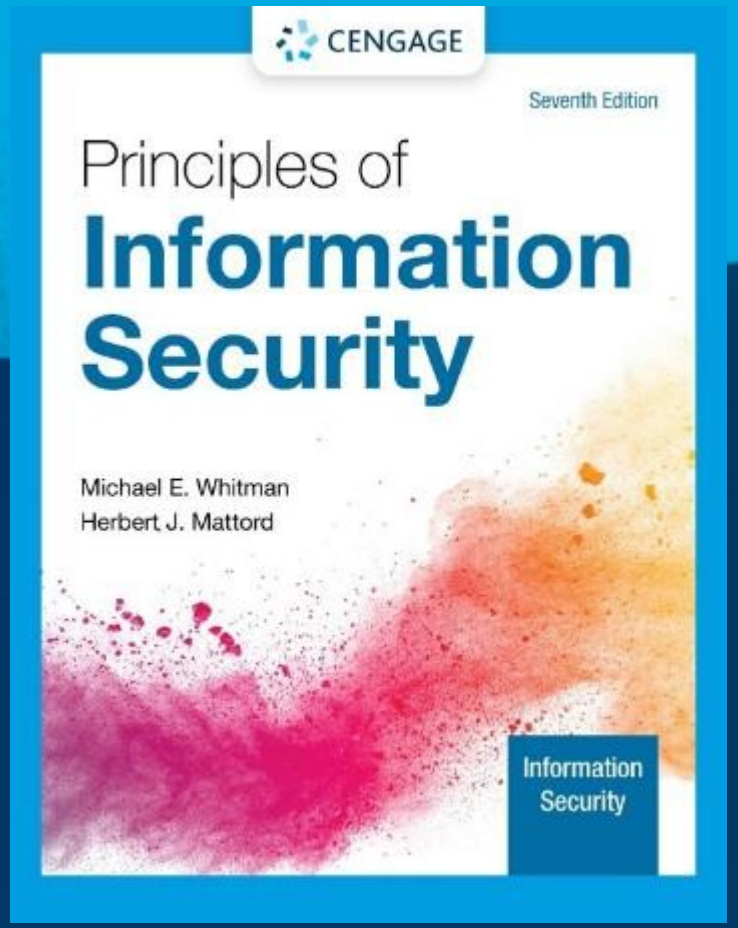

Module 3

Information Security Management

Module Objectives

By the end of this module, you should be able to:

3.1 Describe the different management functions with respect to information security

3.2 Define information security governance and list the expectations of the organization's senior management with respect to it

3.3 Describe management's role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines

3.4 List the elements in an effective security education, training, and awareness program and describe a methodology for effectively implementing security policy in the organization

3.5 Explain what an information security blueprint is, identify its major components, and explain how it supports the information security program

Introduction to the Management of Information Security (1 of 3)

- An information security program begins with policies, standards, and practices, which are the foundation for the information security architecture and blueprint.
- As part of the organization's management team, the InfoSec management team operates like all other management units.

Introduction to the Management of Information Security (2 of 3)

- The InfoSec management team's goals and objectives differ from those of the IT and general management communities in that the InfoSec management team is focused on the secure operation of the organization.
- Some of the InfoSec management team's goals and objectives may be contrary to or require resolution with the goals of the IT management team
- The primary focus of the IT group is to ensure the effective and efficient processing of information.
- The primary focus of the InfoSec group is to ensure the confidentiality, integrity, and availability of information.

Introduction to the Management of Information Security (3 of 3)

- Because InfoSec management oversees a specialized program, certain aspects of its managerial responsibility are unique.
- These unique functions are known as “the six Ps”:
  - Planning
  - Policy
  - Programs
  - Protection
  - People
  - Project management

Information Security Planning and Governance (1 of 2)

- **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**.
- The leadership of the information security function that delivers strategic planning and corporate responsibility is best accomplished using an approach industry refers to as **governance, risk management, and compliance (GRC)**.

Information Security Planning and Governance (2 of 2)

- InfoSec objectives must be addressed at the highest levels of an organization's management team in order to be effective and offer a sustainable approach.
- In organizations with formal boards of directors, the boards should be the basis for **governance** review and oversight.
- **Information security governance** is the application of the principles and practices of corporate governance to the information security function, emphasizing the responsibility of the board of directors and/or senior management for the oversight of information security in the organization.

Information Security Governance (1 of 2)

- ISO 27014:2013: the ISO 27000 series standard for Governance of Information Security—specifies six high-level "action-oriented" information security governance principles:
  1. Establish organization-wide information security.
  2. Adopt a risk-based approach.
  3. Set the direction of investment decisions.
  4. Ensure conformance with internal and external requirements.
  5. Foster a security-positive environment.
  6. Review performance in relation to business outcomes.

ISO/IEC 27014:2013 Governance Processes

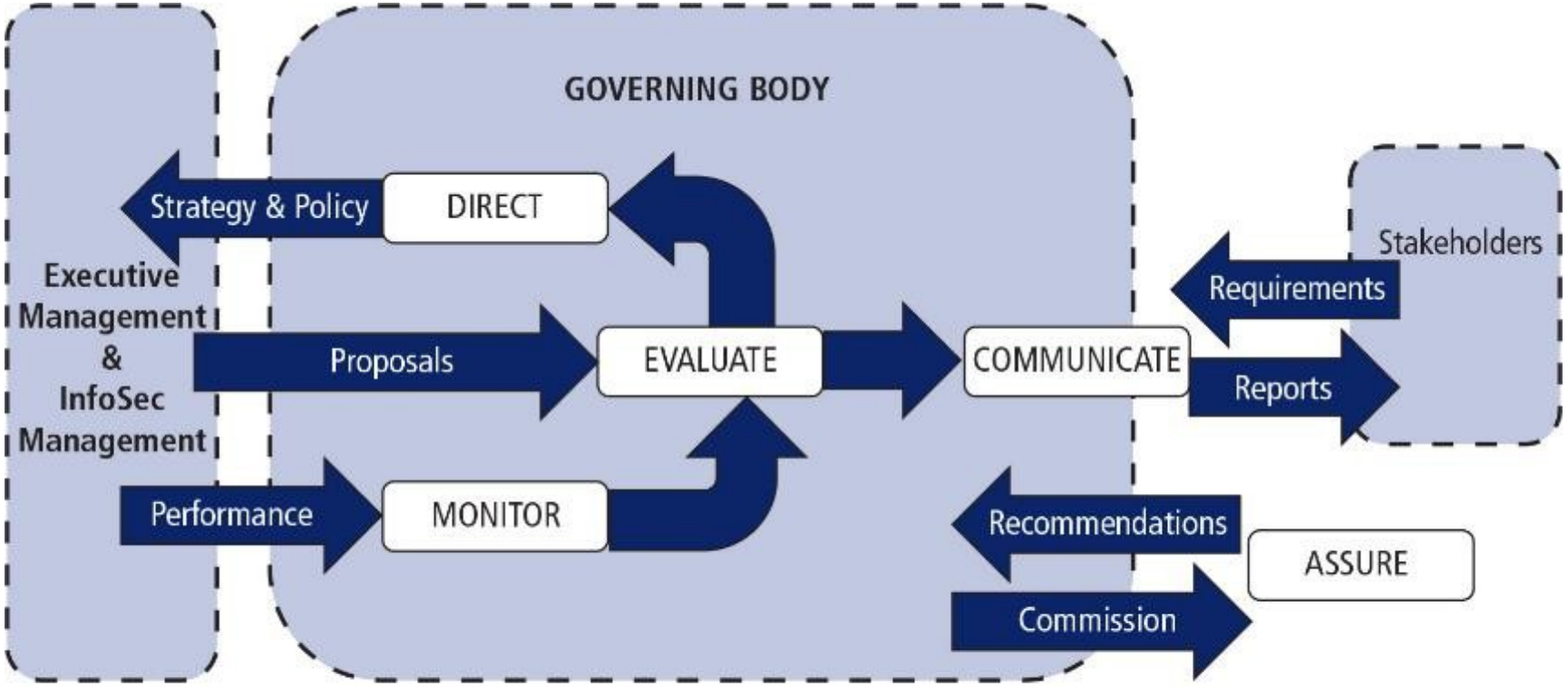

Figure 3-1 ISO/IEC 27014:2013 governance processes[4]

Source: R. Mahncke, Australian eHealth Informatics and Security Conference, December 2013.

Information Security Governance Roles And Responsibilities

Figure 3-2 Information security governance roles and responsibilities

Source: This information is derived from the Corporate Governance Task Force Report, "Information Security Governance: A Call to Action," April 2004, National Cyber Security Task Force.

Information Security Governance (2 of 2)

- Information security governance goals:
  1. Strategic alignment of information security with business strategy to support organizational objectives
  2. Risk management by executing appropriate measures to manage and mitigate threats to information resources
  3. Resource management by using information security knowledge and infrastructure efficiently and effectively
  4. Performance measurement by measuring, monitoring, and reporting information security governance metrics to ensure that organizational objectives are achieved
  5. Value delivery by optimizing information security investments in support of organizational objectives

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 how technologies should be 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 (1 of 2)

- 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.

Policies, Standards, Guidelines, And Procedures

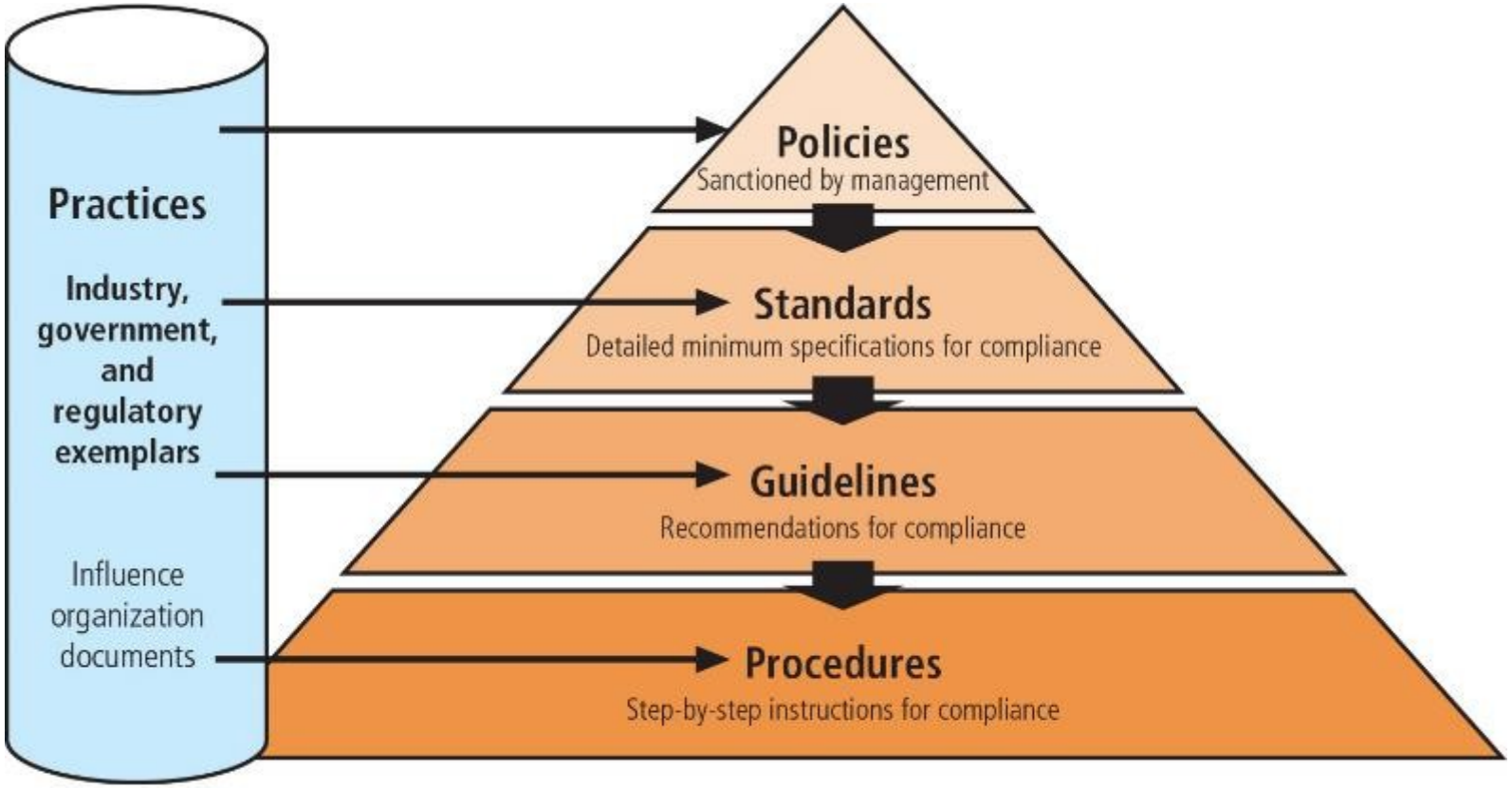

Figure 3-3 Policies, standards, guidelines, and procedures

Relationship between Policies, Standards, Practices, Procedures, and Guidelines

Policy	"Use strong passwords, frequently changed."
Standard	"The password must be at least 10 characters with at least one of each of these: uppercase letter, lowercase letter, number, and special character."
Practice	"According to *Passwords Today*, most organizations require employees to change passwords at least every six months."
Procedure	"In order to change your password, first click the Windows Start button; then ... "
Guideline	"We recommend you don't use family or pet names, or parts of your Social Security number, employee number, or phone number in your password."

Knowledge Check Activity 1

A detailed statement of what must be done to comply with policy, sometimes viewed as the rules governing policy compliance, is known as a(n) _____.

a. guideline

b. standard

c. practice

d. procedure

Knowledge Check Activity 1: Answer

A detailed statement of what must be done to comply with policy, sometimes viewed as the rules governing policy compliance, is known as a(n) _____.

Answer: b. standard

Standards are more detailed statements of what must be done to comply with policy. Standards may be informal or part of an organizational culture or standards may be published. Practices, procedures, and guidelines effectively explain how to comply with policy.

Policy as the Foundation for Planning (2 of 2)

- **An information security policy** provides rules for protection of the organization's information assets.
- Management must define three types of security policy:
  1. Enterprise information security policies
  2. Issue-specific security policies
  3. Systems-specific security policies

Enterprise Information Security Policy (EISP) (1 of 2)

- 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) (2 of 2)

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

Components of the EISP (1 of 3)

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."

Components of the EISP (2 of 3)

Component	Description
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.

Components of the EISP (3 of 3)

Component	Description
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.

Issue-Specific Security Policy (ISSP)

- The ISSP:
  1. Addresses specific areas of technology
  2. Requires frequent updates
  3. Contains statement on the organization's position on a specific issue
- Three common approaches when creating and managing ISSPs:
  - Independent ISSP documents, each tailored to a specific issue
  - A single comprehensive ISSP document that covers all issues
  - A modular ISSP document that unifies policy creation and administration while maintaining each specific issue's requirements

Components of an ISSP (1 of 3)

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

Components of an ISSP (2 of 3)

Components of an ISSP
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

Components of an ISSP (3 of 3)

Components of an ISSP
7. Limitations of liability a. Statements of liability b. Other disclaimers as needed

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.

Developing and Implementing Effective Security Policy

For policies to be effective and legally defensible, the following must be done properly:

1. Development—They must be written using industry-accepted practices and formally approved by management.
2. Dissemination—They must be distributed using all appropriate methods.
3. Reading—They must be reviewed by all employees.
4. Comprehension—They must be understood by all employees.
5. Compliance—They must be formally agreed to by act or affirmation.
6. Enforcement—They must be uniformly applied to all employees.

Policy Management

- Policies must be managed, as they constantly change.
- To remain viable, security policies must have:
  - Responsible manager/policy administrator
  - Schedule of reviews
  - Review procedures and practices
  - Policy and revision dates
  - Automated policy management

Security Education, Training, and Awareness Program

- Once general security policy exists, implement a **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.
- SETA 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 security.
- When formal education is deemed appropriate, an employee can investigate degree programs or courses in continuing education from local institutions of higher learning.
- Resources, such as the DHS/NSA-designated National Centers of Academic Excellence program (www.iad.gov/NIETP/index.cfm), can provide additional information on security curriculum.

Security Training

- 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.
- Massive Open Online Courses (MOOCs) are available from vendors such as Coursera (www.coursera.org), with free courses and completion certificates for a nominal fee.

Security Awareness

- Security awareness program: one of the least frequently implemented but most beneficial programs
- 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

Comparative Framework of SETA (1 of 2)

	Awareness	Training	Education
Attribute	Seeks to teach members of the organization *what* security is and what the employee should do in some situations	Seeks to train members of the organization *how* they should react and respond when threats are encountered in specified situations	Seeks to educate members of the organization as to *why* it has prepared in the way it has and why the organization reacts in the ways it does
Level	Offers basic *information* about threats and responses	Offers more detailed *knowledge* about detecting threats and teaches skills needed for effective reaction	Offers the background and depth of knowledge to gain *insight* into how processes are developed and enables ongoing Improvement

Comparative Framework of SETA (2 of 2)

	Awareness	Training	Education
Objective	Members of the organization can *recognize* threats and formulate simple responses	Members of the organization can mount effective responses using learned *skills*	Members of the organization can engage in active defense and use *understanding* of the organization's objectives to make continuous improvement
Teaching methods	• Media videos • Newsletters • Posters • Informal training	• Formal training • Workshops • Hands-on practice	• Theoretical instruction • Discussions/seminars • Background reading
Assessment	True/false or multiple choice (identify learning)	Problem solving (apply learning)	Essay (interpret learning)
Impact time frame	Short-term	Intermediate	Long-term

Knowledge Check Activity 2

The process that seeks to teach members of the organization what security is and what the employee should do in some situations is known as security _____.

a. education

b. training

c. awareness

d. alertness

Knowledge Check Activity 2: Answer

The process that seeks to teach members of the organization what security is and what the employee should do in some situations is known as security _____.

Answer: c. awareness

Training is how an organization prepares members on how they should react and respond when threats are encountered in specified situations. Education seeks to provide theoretical foundations to members of the organization as to why it has prepared in the way it has and why the organization reacts in the ways it does. Alertness is not an element covered in this module.

Information Security Blueprint, Models, and Frameworks

- The **information security blueprint** is the basis for design, selection, and implementation of all security elements.
- The blueprint is the organization's detailed implementation of an **information security framework** and specifies tasks and the order in which they are to be accomplished.
- An **information security framework** is the specification to be followed during the design, selection, and implementation of security controls.
- An **information security model** is a well-recognized framework promoted by a government agency, standards organization, or industry group.
- *Framework* and *model* are sometimes used interchangeably.

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 with the goal of certification
- Provides a starting point for developing organizational security

ISO/IEC 27001:2013 Major Process Steps

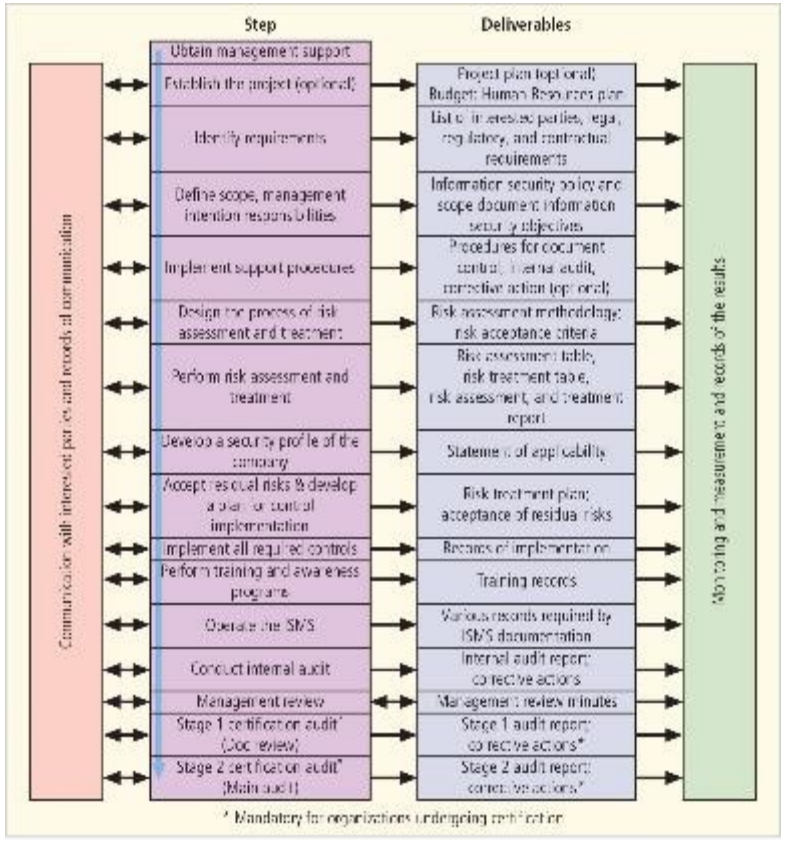

Figure 3-9 ISO/IEC 27001:2013 major process steps[22]

Source: 27001 Academy; ISO 27001 and ISO 31001 Online Consultation Centre.

The Sections of ISO/IEC 27002:2013 (1 of 2)

ISO 27002:2013 Contents
Foreword
0. Introduction
1. Scope
2. Normative references
3. Terms and definitions
4. Structure of this standard
5. Information security policies
6. Organization of information security
7. Human resource security
8. Asset management

The Sections of ISO/IEC 27002:2013 (2 of 2)

ISO 27002:2013 Contents
9. Access control
10. Cryptography
11. Physical and environmental security
12. Operations security
13. Communication security
14. System acquisition, development, and maintenance
15. Supplier relationships
16. Information security incident management
17. Information security aspects of business continuity management
18. Compliance

NIST Security Models (1 of 2)

- Another possible approach described in the documents available from Computer Security Resource Center of NIST
  - SP 800-12, Rev. 1: “An Introduction to Information Security”
  - SP 800-18, Rev. 1: “Guide for Developing Security Plans for Federal Information Systems”
  - SP 800-30, Rev. 1: “Guide for Conducting Risk Assessments”
  - SP 800-37, Rev. 2: “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy”
  - SP 800-39: “Managing Information Security Risk: Organization, Mission, and Information System View”

NIST Security Models (2 of 2)

- Another possible approach described in the documents available from Computer Security Resource Center of NIST
  - 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”

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

NIST and the Risk Management Framework

- NIST's approach to managing risk in the organization, titled the Risk Management Framework (RMF), emphasizes:
  - Building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls
  - Maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes
  - Providing essential information to help senior leaders make decisions about accepting risk to an organization's operations and assets, individuals, and other organizations arising from the use of information systems

NIST Cybersecurity Framework (1 of 2)

- Consists of three fundamental components:
  - Framework core: set of information security activities an organization is expected to perform and their desired results:
    - Identify
    - Protect
    - Detect
    - Respond
    - Recovery

NIST Cybersecurity Framework (2 of 2)

- Consists of three fundamental components:
  - Framework tiers: help relate the maturity of security programs and implement corresponding measures and functions
    - Tier 1: Partial
    - Tier 2: Risk Informed
    - Tier 3: Repeatable
    - Tier 4: Adaptive
  - Framework profile: used to perform a gap analysis between the current state and a desired state of information security/risk management

NIST Cybersecurity Framework

- Seven-step approach to implementing/improving programs:
  1. Prioritize and scope
  2. Orient
  3. Create current profile
  4. Conduct risk assessment
  5. Create target profile
  6. Determine, analyze, prioritize gaps
  7. 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 the 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 security, 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.

Knowledge Check Activity 3

Information security safeguards focus on lower-level planning that deale with the functionality of the organization's security; they include disaster recovery planning, incident response planning, and SETA programs and are collectively called _____ controls.

a. managerial

b. technical

c. strategic

d. operational

Knowledge Check Activity 3: Answer

Information security safeguards focus on lower-level planning that deal with the functionality of the organization's security; they include disaster recovery planning, incident response planning, and SETA programs and are collectively called _____ controls.

Answer: d. operational

Operational controls address personnel and physical security and the protection of production inputs/outputs, while managerial controls set the direction and scope of the security processes and provide detailed instructions for their conduct, and technical controls are the tactical and technical implementations related to designing and integrating security in the organization.

Spheres of Security

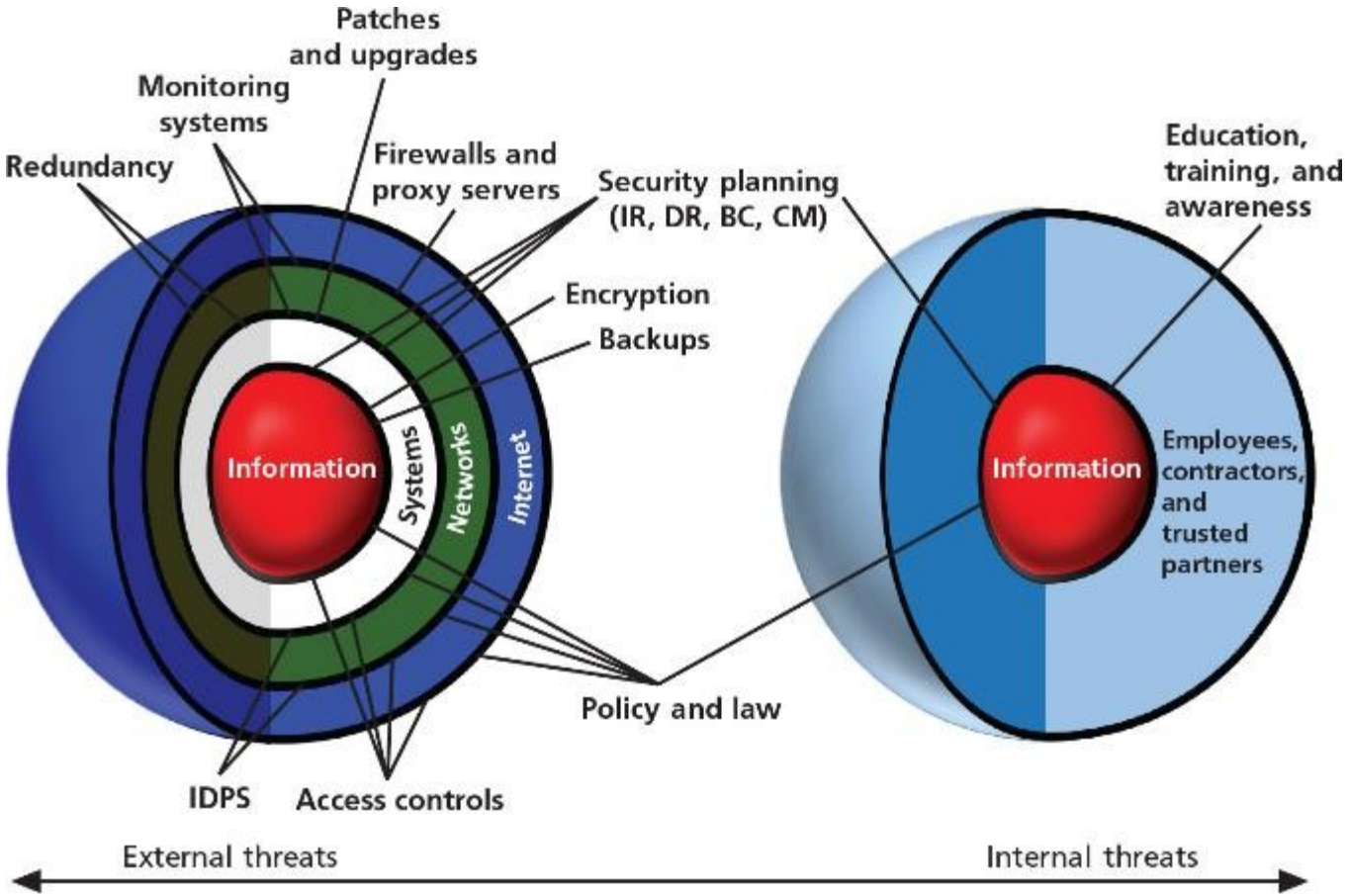

Figure 3-10 Spheres of security

Design of Security Architecture

- Defense in depth
  - Implementation of security in layers
  - Requires that organizations 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 on-site physical threats

Defense in Depth

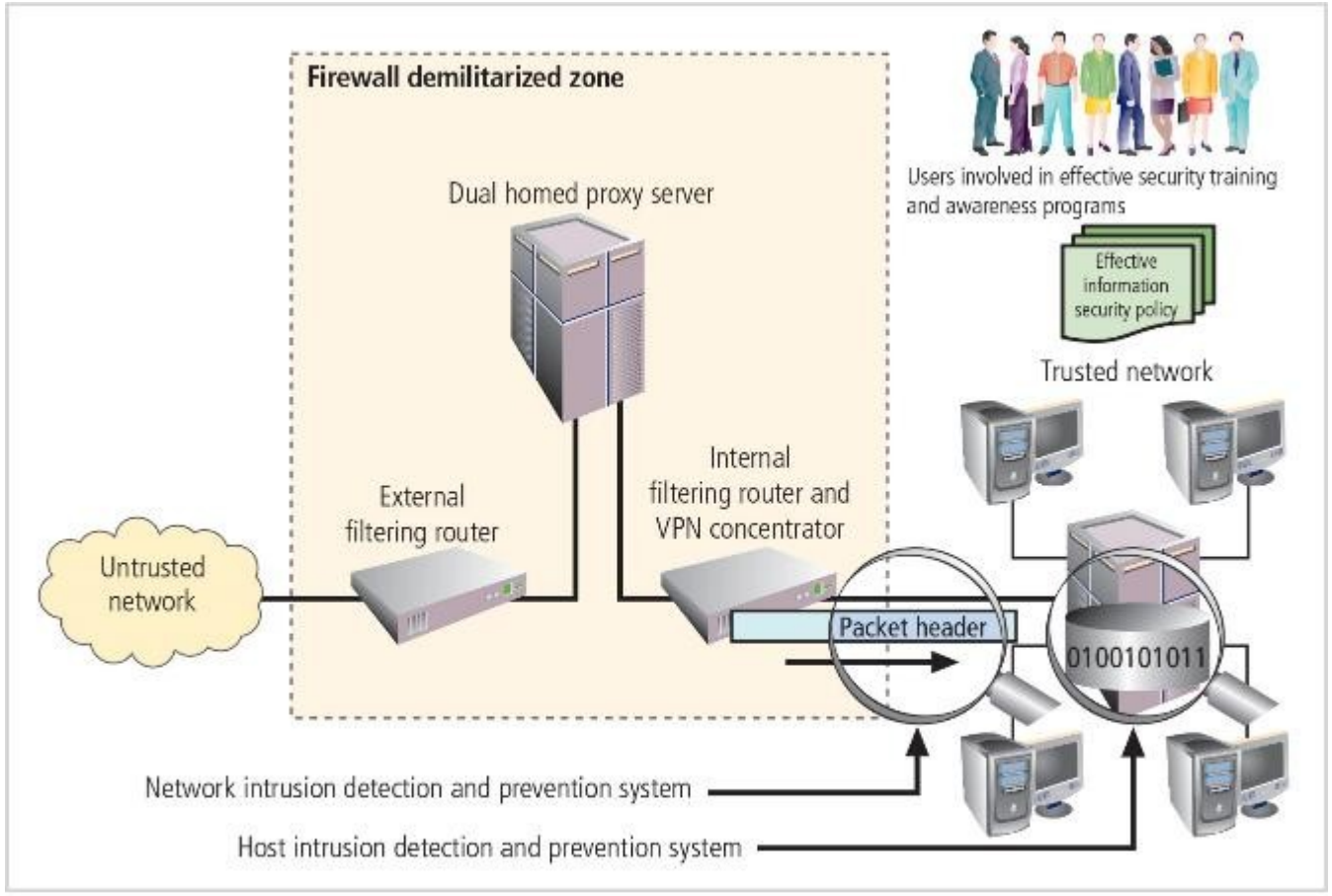

Figure 3-11 Defense in depth

Security Perimeters and Domains

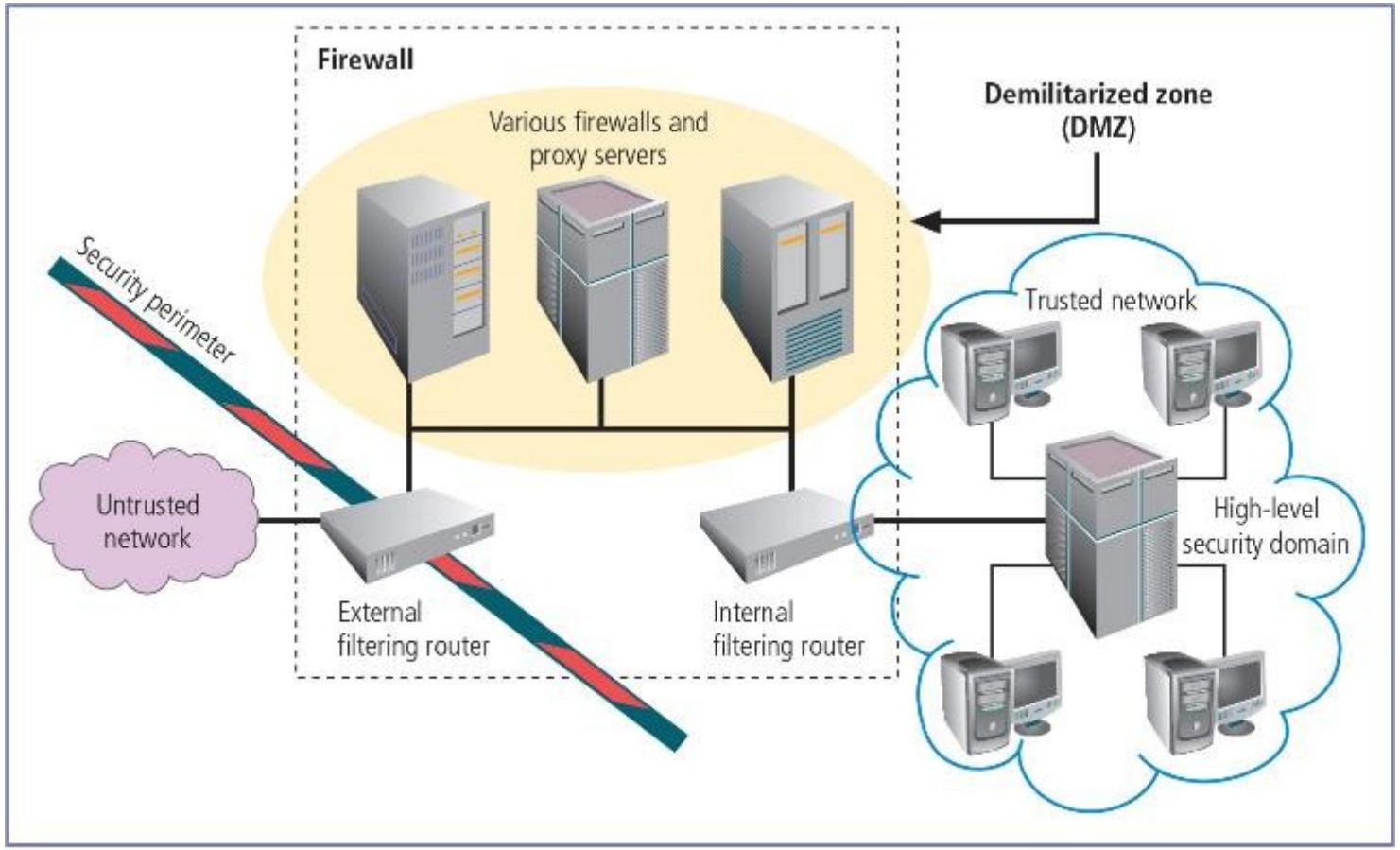

Figure 3-12 Security perimeters and domains

Summary (1 of 3)

- 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.
- Standards are more detailed than policies and describe the steps that must be taken to conform to policies.

Summary (2 of 3)

- Management must define three types of security policies: general or security program policies, issue-specific security policies, and systems-specific security policies.
- The enterprise information security policy (EISP) should be a driving force in the planning and governance activities of the organization as a whole.
- 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.

Summary (3 of 3)

- Several published information security frameworks by government organizations, private organizations, and professional societies supply information on best practices for their members.
- One of the foundations of security architectures is the layered implementation of security. This layered approach is referred to as defense in depth.
- Several published information security frameworks by government organizations, private organizations, and professional societies supply information on best practices for their members.
- One of the foundations of security architectures is the layered implementation of security. This layered approach is referred to as defense in depth.

Self-Assessment (1 of 2)

- Look early in the module for the list of the six Ps.
- These elements, (planning, policy, programs, protection, people, and project management) are discussed in this module in ways unique to information security, although most of them also apply to general management.
- In your opinion, which of these elements stood out for you as capturing the *essence* of information security? Why?

Self-Assessment (2 of 2)

- Governance is about keeping business systems *in control*.
- Can you think of a situation when information security governance and corporate governance might be in conflict?
- How do you think that will be resolved?