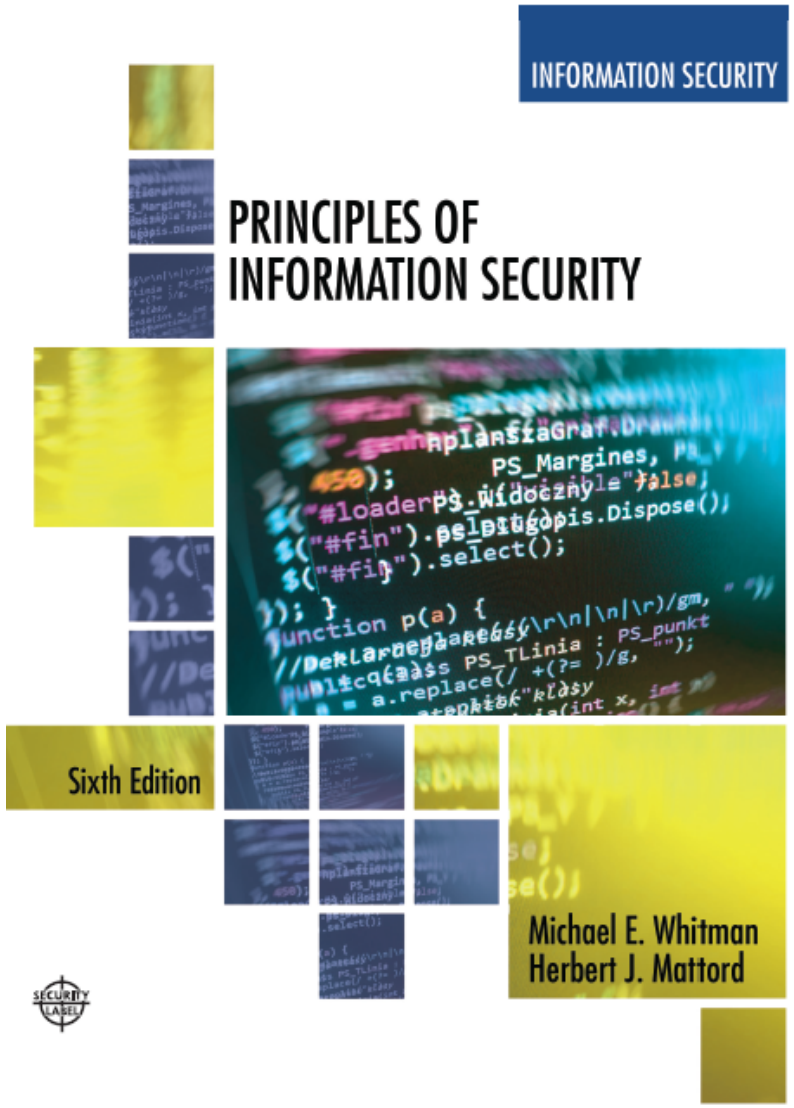


Source: Principles of Information Security

Chapter 4

Planning for Security

Dr. Ibrahim Waziri Jr.

Learning Objectives

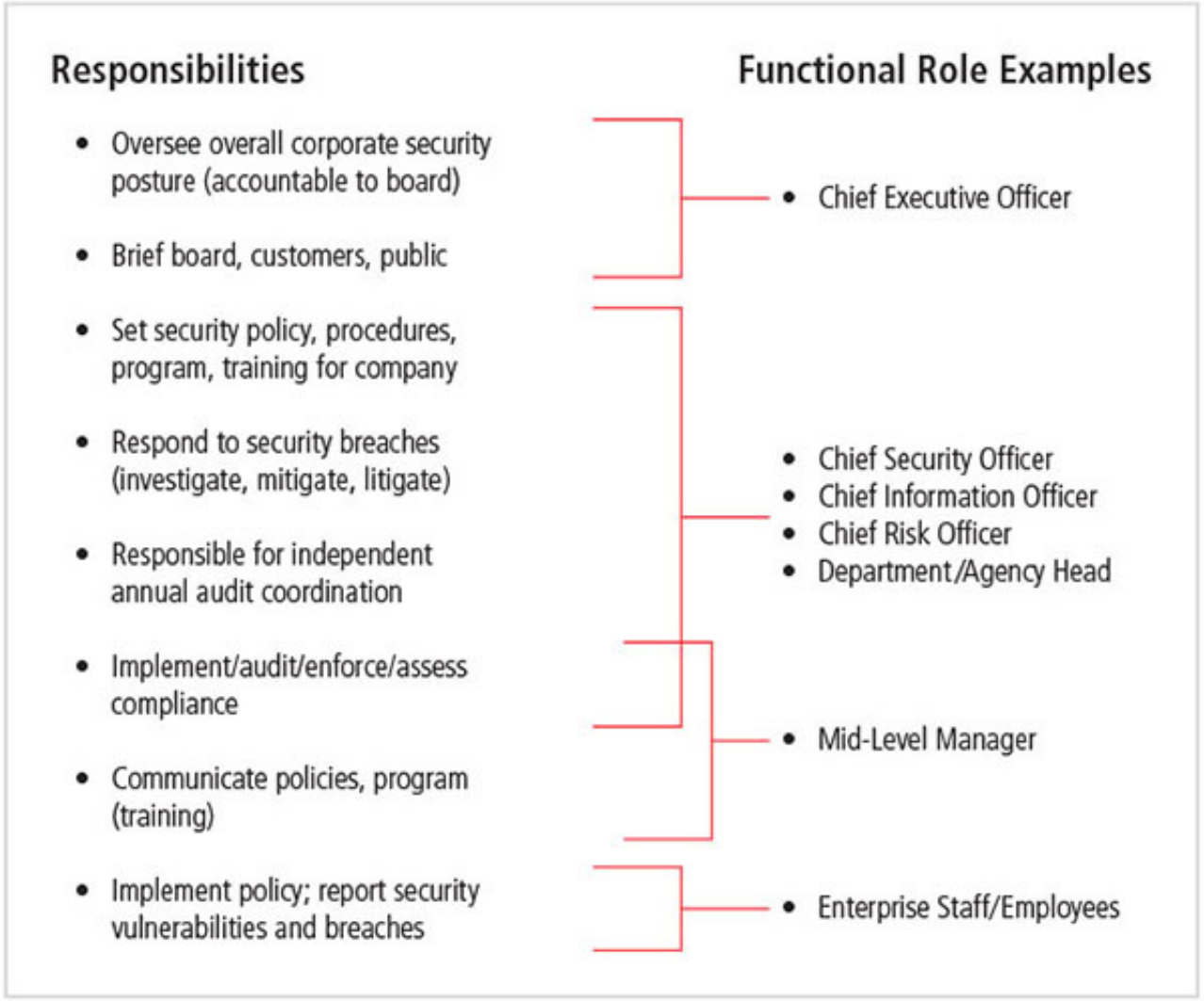
Upon completion of this material, you should be able to:

- 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
- 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



Governance: Set of responsibilities and practices exercised by the board and executive management.

Information security governance outcomes – Five Goals:

- Strategic alignment
- Risk management
- Resource management
- Performance measurement
- Value delivery

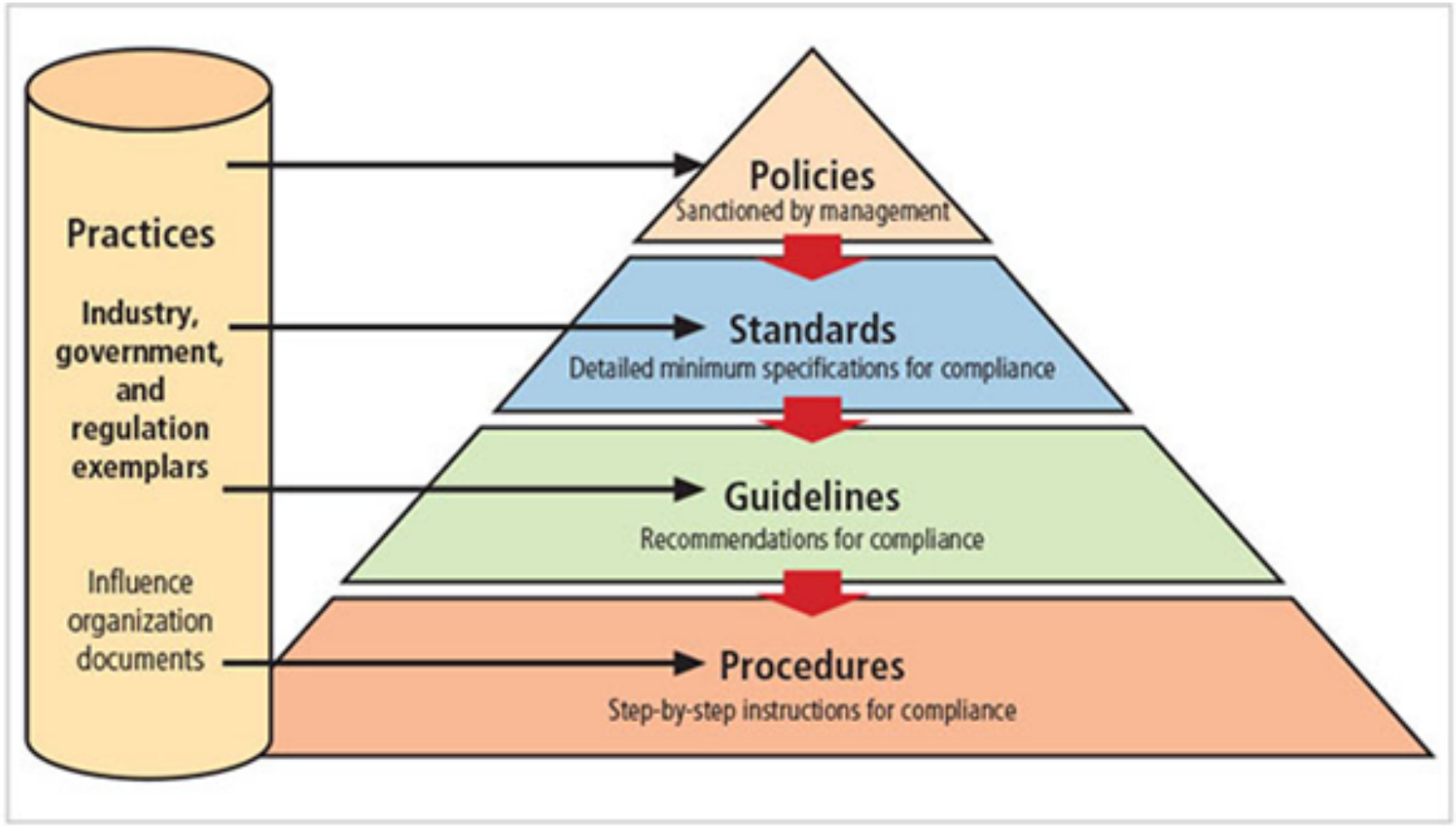
Information Security Policy, Standards, and Practices

- 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.

Policy as the Foundation for Planning



Enterprise Information Security Policy (EISP)

Sets strategic direction, scope, and tone for all security efforts within the organization

EISP Elements should include:

- Overview of the 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

Components of EISP:

- Statement of Purpose
- Information Security Components
- Need for Information Security
- Information Security Roles and Responsibilities
- Reference Standards to Other Information and Guidelines

Issue-Specific Security Policy (ISSP)

The ISSP addresses specific areas of technology, requires frequent update, and 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

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

Systems-Specific Security Policy (SysSP)

SysSPs often function as standards or procedures used when configuring or maintaining systems.

SysSPs fall into two groups:

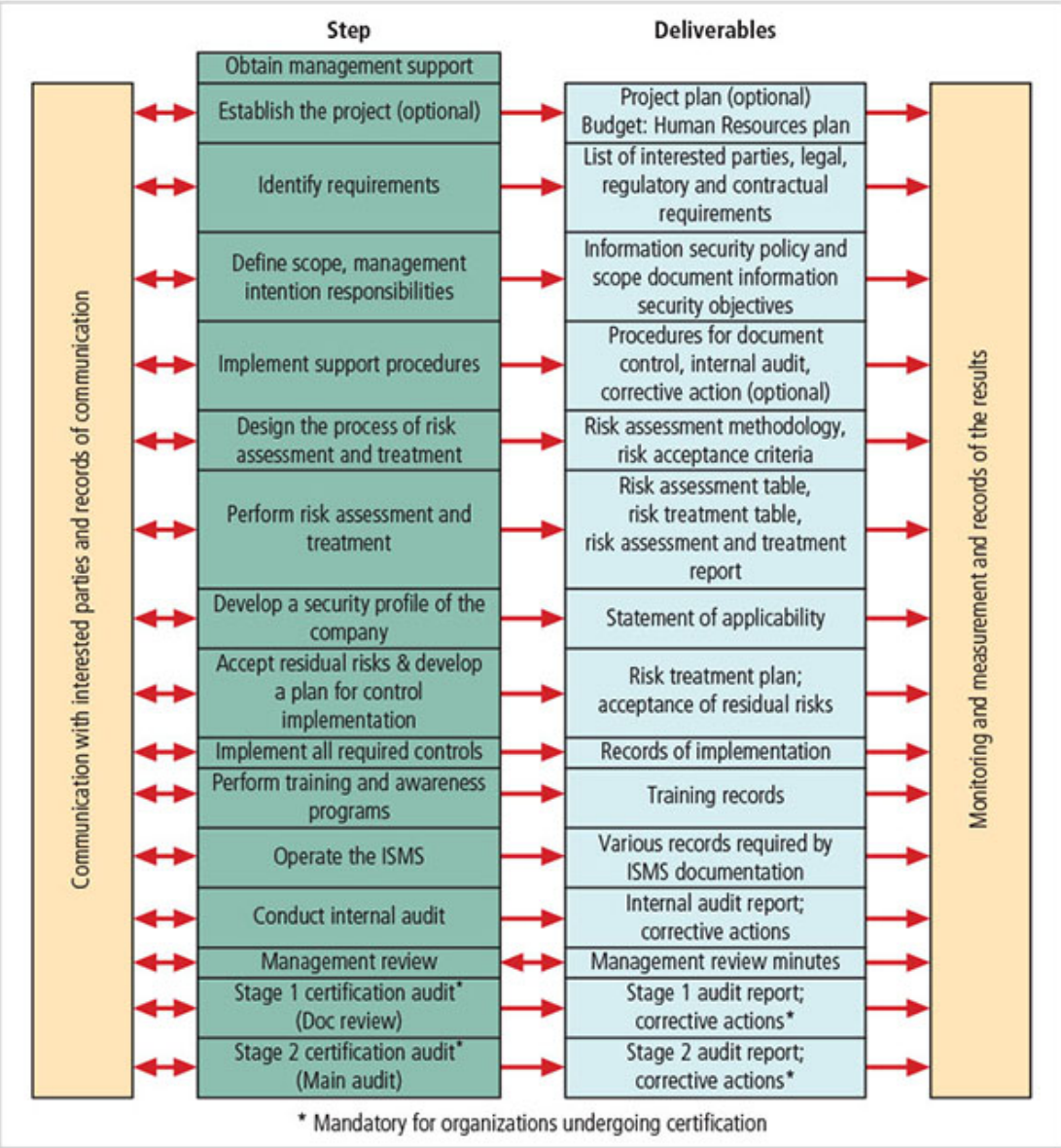
- Managerial guidance
- Technical specifications
  - Access control lists (ACLs) can restrict access for a particular user, computer, time, duration—even a particular file.
  - Configuration rule policies govern how a security system reacts to received data.

Combination SysSPs combine managerial guidance and technical specifications.

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

NIST Special Publications

Another approach available is described in the many documents available from the Computer Security Resource Center of the National Institute for Standards and Technology (csrc.nist.gov).

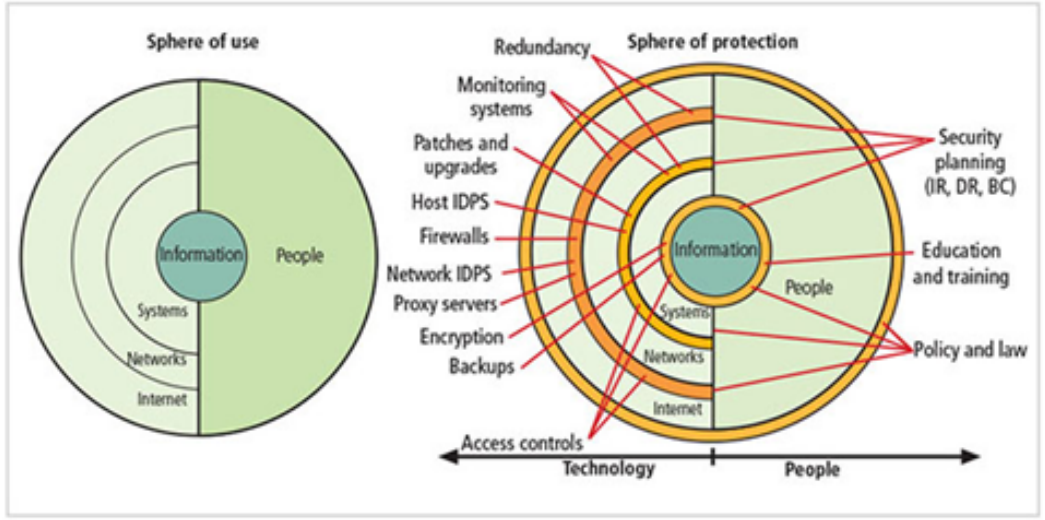
NIST Cybersecurity Framework - Consists of three fundamental components:

- Framework core
- Framework tiers
- Framework profile

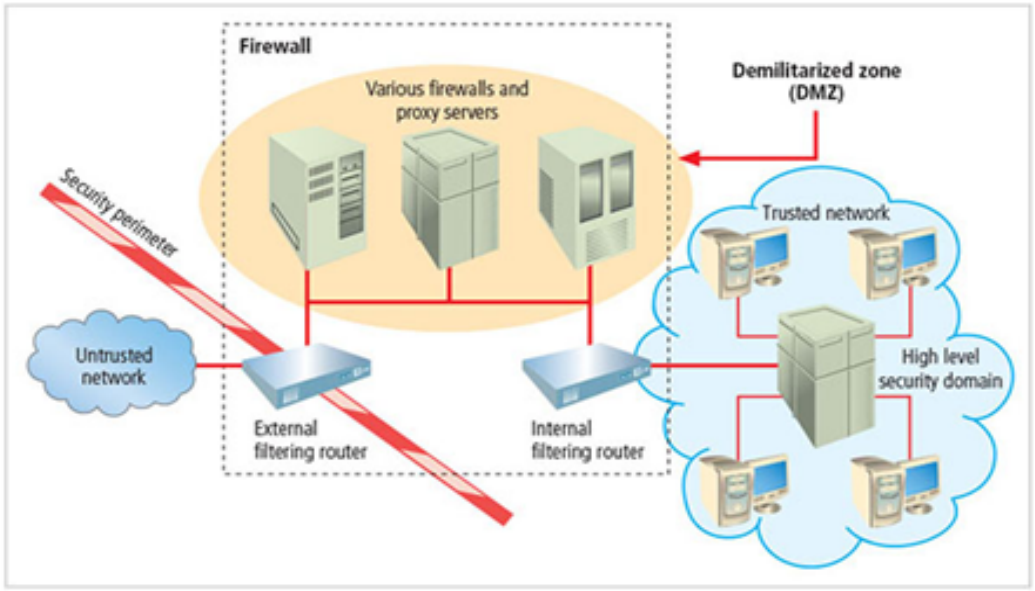
Seven-step approach to implementing/improving programs:

- Prioritize and scope
- Orient
- Create current profile
- Conduct risk assessment
- Create target profile
- Determine, analyze, and prioritize gaps
- Implement action plan

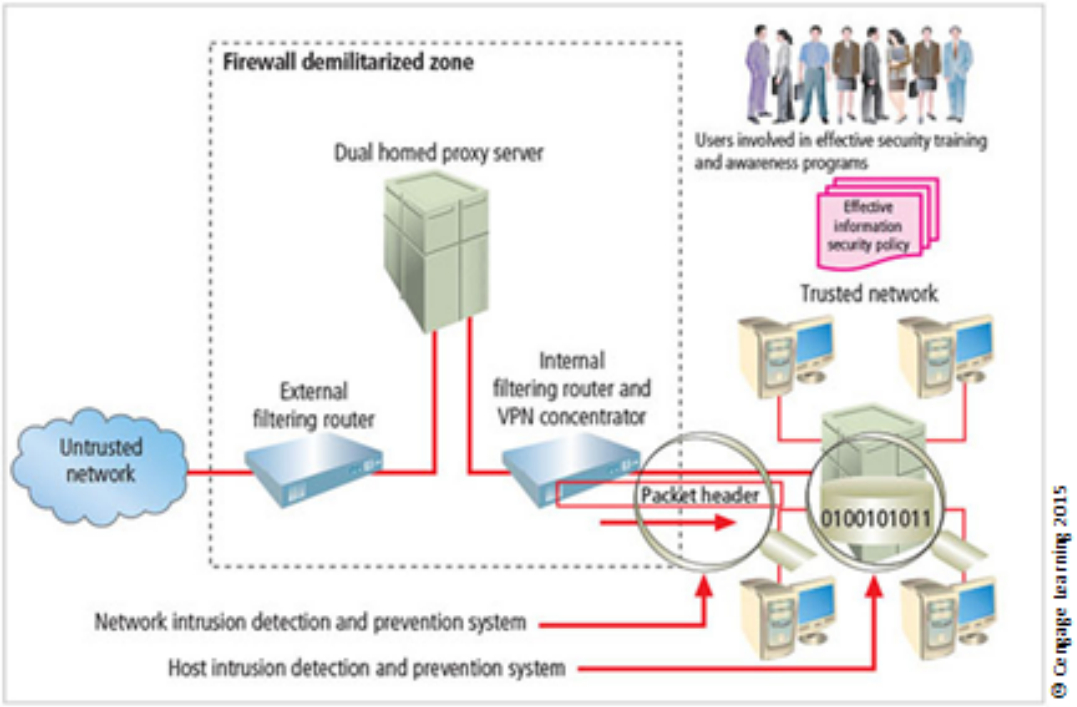
Design of Security Architecture



Spheres of security



Security perimeter



Defense in depth

Security Education, Training, and Awareness (SETA)

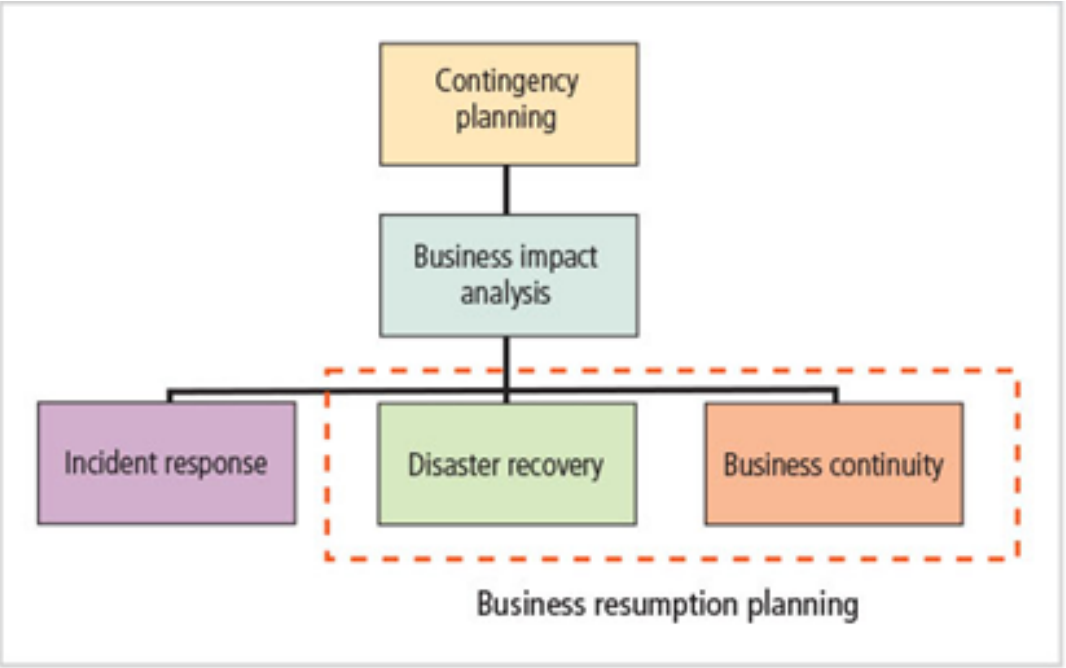
Once general security policy exists, implement security education, training, and awareness (SETA) program.

- SETA is a control measure designed to reduce accidental security breaches.
- The SETA program consists of security education, security training, and security awareness.
- It enhances security by improving awareness, developing skills and knowledge, and building in-depth knowledge.

Continuity Strategies

Incident response plans (IRPs), disaster recovery plans (DRPs), and business continuity plans (BCPs)

- IRP focuses on immediate response.
- DRP typically focuses on restoring systems after disasters occur.
- BCP occurs concurrently with DRP when damage is major or ongoing.



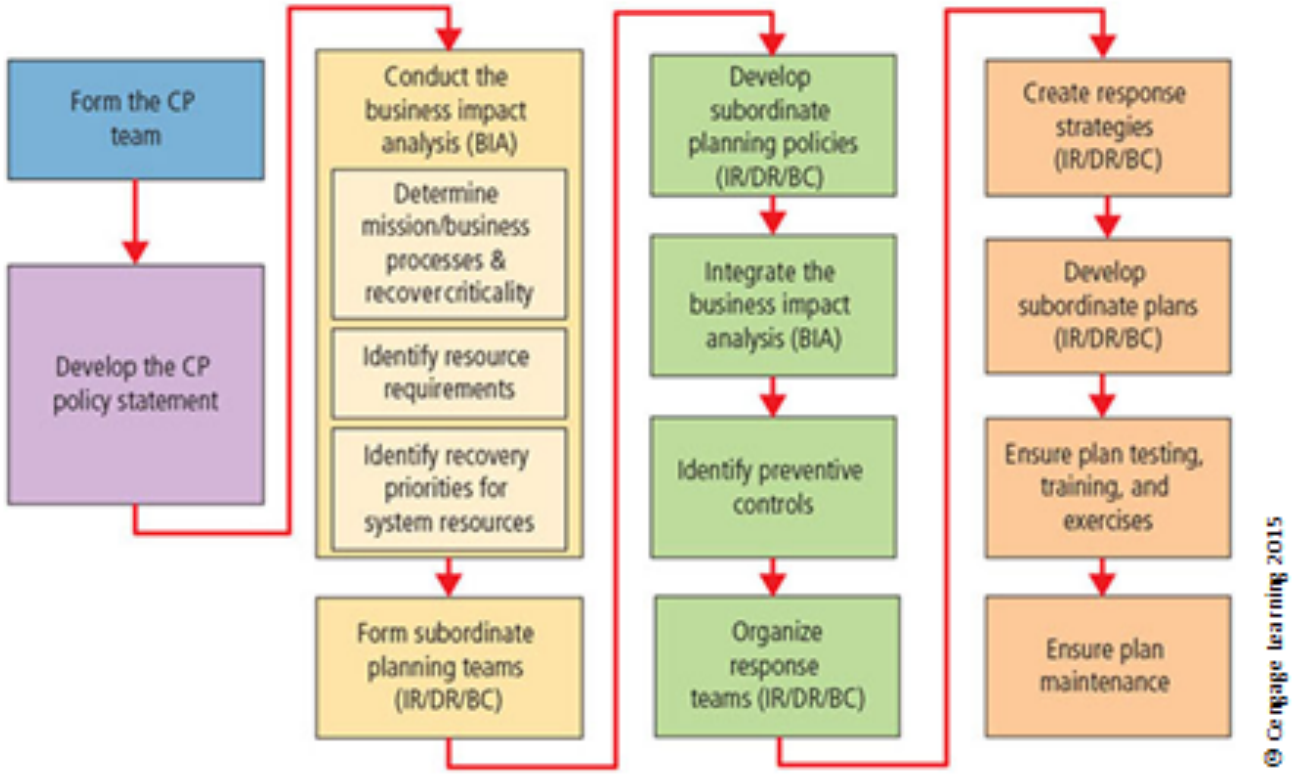
Contingency Planning Team: Before planning can actually begin, a team has to start the process:

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.

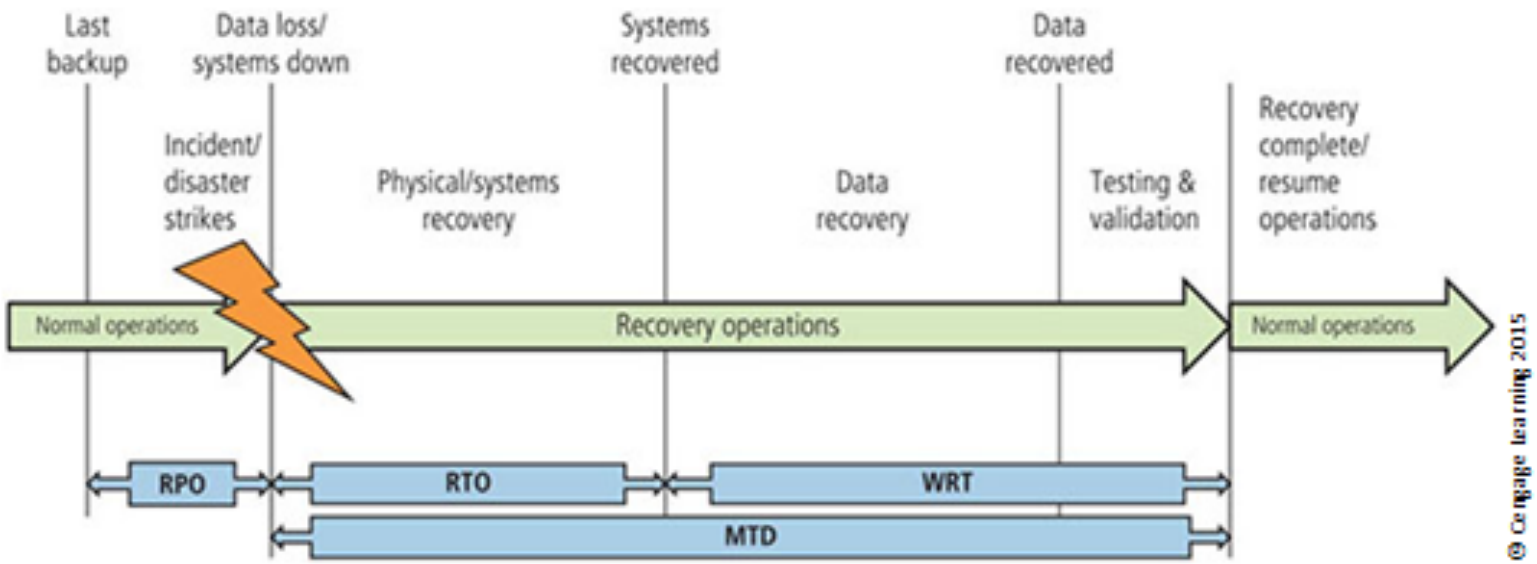
Team members: from various communities of interest: business, IT, and information security.

Contingency Planning (CP) Process



- 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

Business Impact Analysis (BIA)



Three stages:

- Determine mission/business processes and recovery criticality
- Identify recovery priorities for system resources
- Identify resource requirements

- Investigation and assessment of various adverse events that can affect organization
- Assumes security controls have been bypassed, have failed, or have proven ineffective, and the attack has succeeded
- Organization should consider scope, plan, balance, knowledge of objectives, and follow-ups

Incident Response Planning (IRP)

Incident response planning includes identification of, classification of, and response to an incident. Incident response 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.

IR Process:

- Incident Planning
- Incident response plan
- Incident detection
- Incident reaction
- Incident containment strategies
- Incident recovery
- Damage assessment
- Automated response

IR policy identifies the following 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

Disaster Recovery Planning (DRP)

- 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 (BCP)

BCP prepares the organization to reestablish or relocate critical business operations during a disaster that affects operations at the primary site.

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.
- There are three shared functions: time-share, service bureaus, and mutual agreements.

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.

Crisis Management

Actions taken in response to an emergency should minimize injury/loss of life, preserve organization's image/market share, and complement disaster recovery/business continuity processes.

Disaster recovery personnel must know their roles without any supporting documentation.

- Preparation
- Training
- Rehearsal

Crisis management team is responsible for managing the event from an enterprise perspective and covers:

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.

There are pros and cons to law enforcement involvement.

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.
- 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).