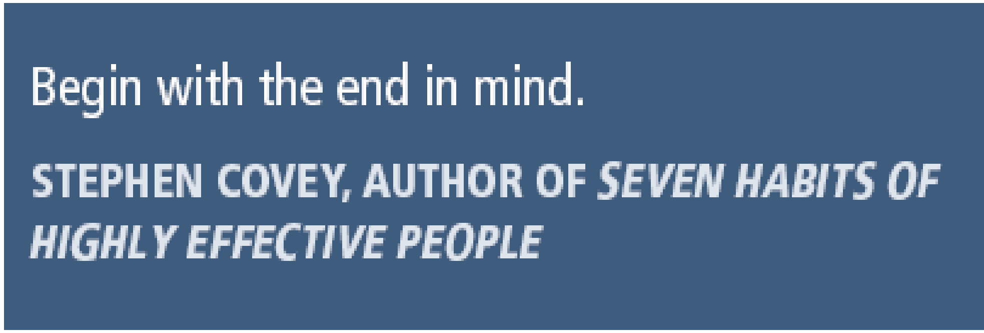
Principles of Information Security

Chapter 5

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:
  - Define management’s role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines
  - Describe 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 and training programs
- Explain what contingency planning is and how it relates to incident response planning, disaster recovery planning, and business continuity plans

Introduction

- Creation of information security program begins with creation and/or review of an organization’s information security policies, standards, and practices
- Then, selection or creation of information security architecture and the development and use of a detailed information security blueprint creates a plan for future success
- Without policy, blueprints, and planning, an organization is unable to meet information security needs of various communities of interest

Information Security Policy

- Communities of interest must consider policies as the basis for all information security efforts
- Policies direct how issues should be addressed and technologies used
- Policies should never contradict law
- Security policies are the least expensive controls to execute but most difficult to implement properly

Definitions

- Policy: course of action used by organization to convey /send instructions from management to those who perform duties
- Policies are organizational laws
- 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/distributed, read, understood, and agreed to by all members of organization and uniformly enforced

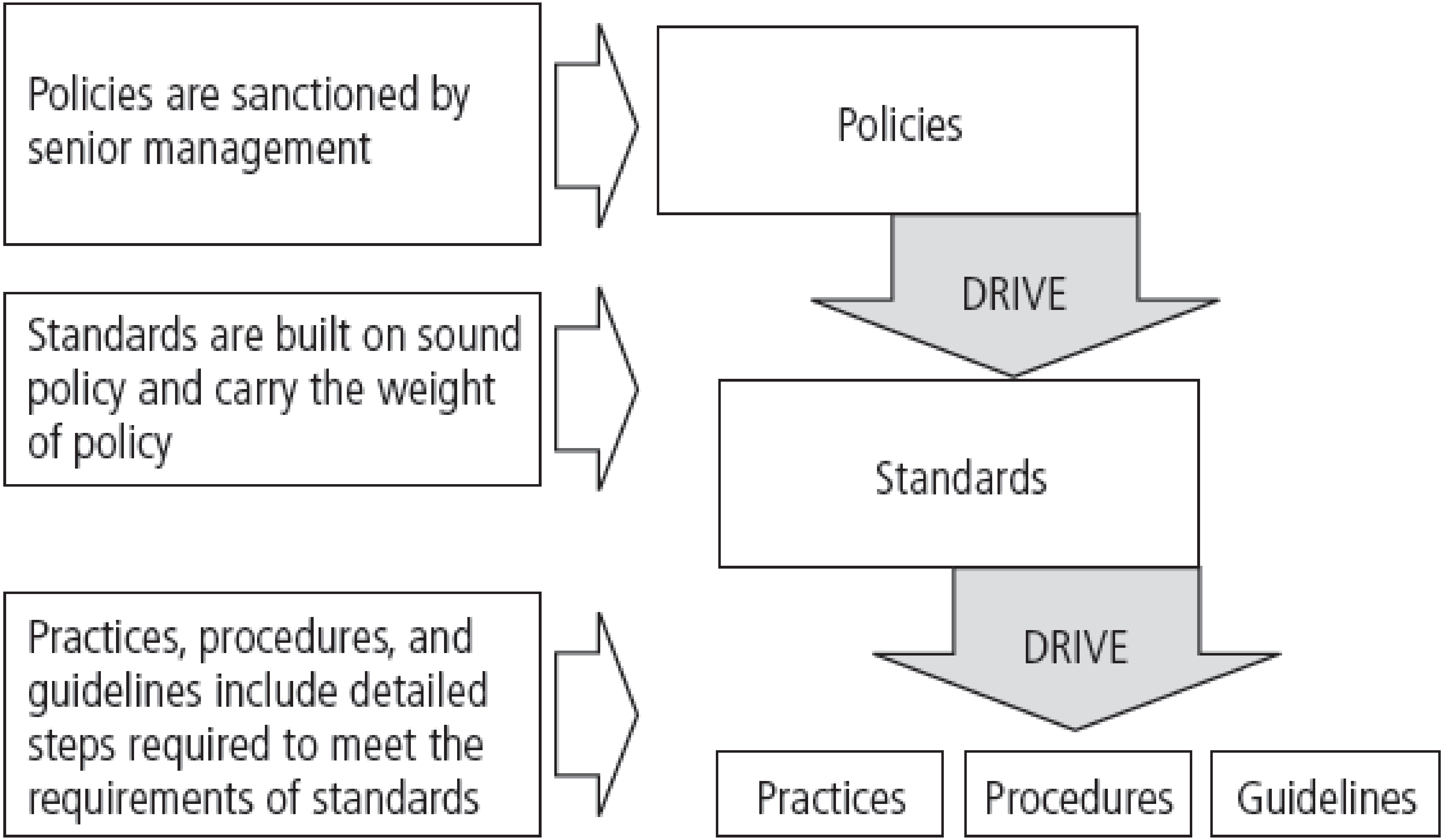

Policies are sanctioned by senior management
Standards are built on sound policy and carry the weight of policy
Practices, procedures, and guidelines include detailed steps required to meet the requirements of standards
Policies
DRIVE
Standards
DRIVE
Practices
Procedures
Guidelines

Figure 5-1 Policies, Standards, and Practices

General or security program policy

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

Issue-Specific Security Policy (ISSP)

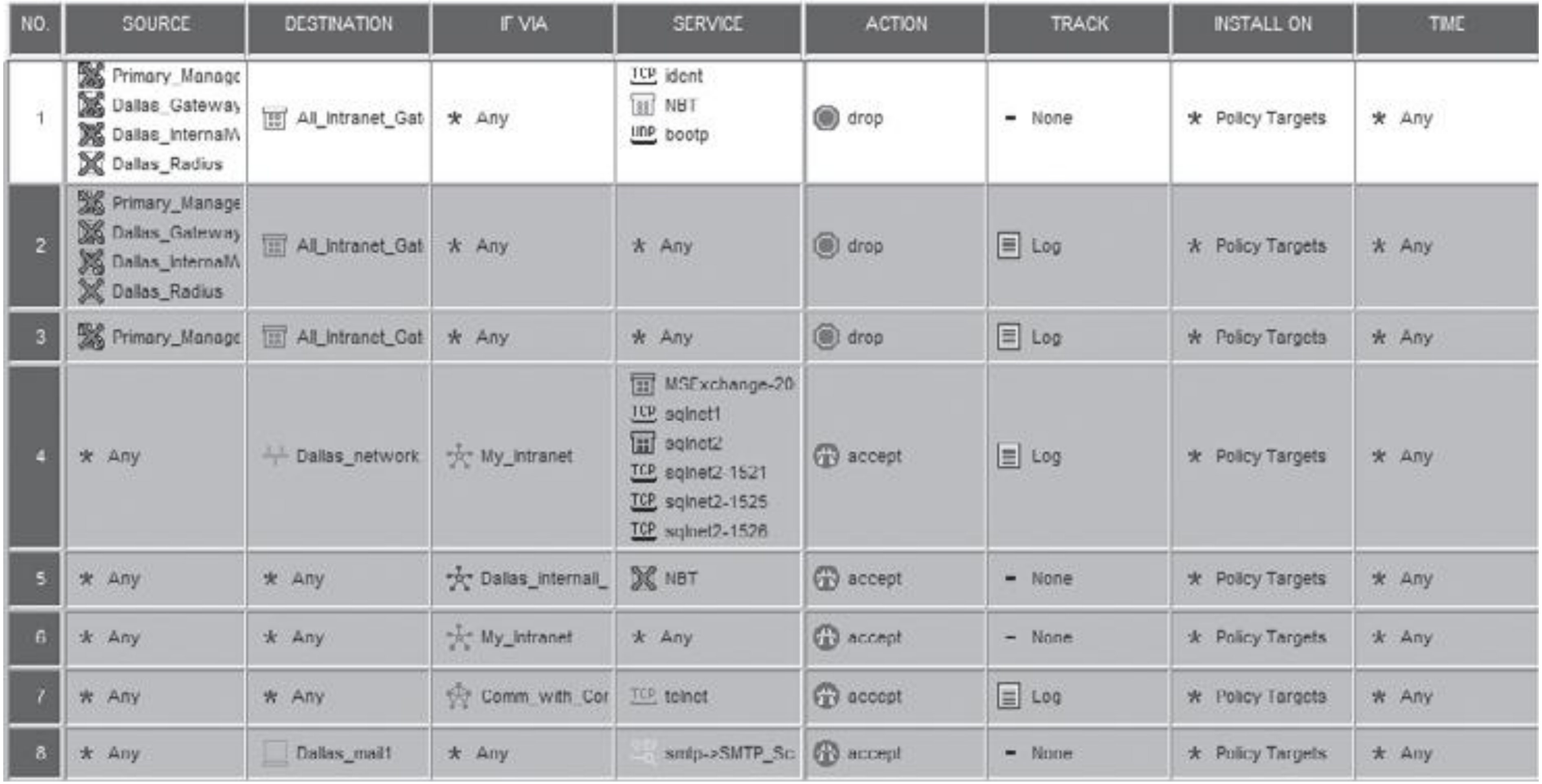
- The ISSP:
  - Addresses specific areas of technology
  - Requires frequent updates
  - Contains statement on organization’s position on specific issue
- Three approaches when creating and managing ISSPs:
  - Create a number of independent ISSP documents
  - Create a single comprehensive ISSP document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

Systems-Specific Policy (SysSP)

- SysSPs frequently function as standards and procedures used when configuring or maintaining systems
- Systems-specific policies fall into two groups
  - Managerial guidance
  - Technical specifications
- ACLs can restrict access for a particular user, computer, time, duration—even a particular file
- Configuration rule policies
- Combination SysSPs



NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	Primary_Managc Dallas_Gateway Dallas_InternalV Dallas_Radius	All_Intranet_Gat	* Any	ident NBT bootp	drop	- None	* Policy Targets	* Any
2	Primary_Manage Dallas_Gateway Dallas_InternalV Dallas_Radius	All_Intranet_Gat	* Any	* Any	drop	Log	* Policy Targets	* Any
3	Primary_Managc	All_Intranet_Gat	* Any	* Any	drop	Log	* Policy Targets	* Any
4	* Any	Dallas_network	My_Intranet	MSExchange-20 sqlnet1 sqlnet2 sqlnet2-1521 sqlnet2-1525 sqlnet2-1526	accept	Log	* Policy Targets	* Any
5	* Any	* Any	Dallas_internal_	NBT	accept	- None	* Policy Targets	* Any
6	* Any	* Any	My_Intranet	* Any	accept	- None	* Policy Targets	* Any
7	* Any	* Any	Comm_with_Cor	telnet	accept	Log	* Policy Targets	* Any
8	* Any	Dallas_mail1	* Any	smtp->SMTP_Sc	accept	- None	* Policy Targets	* Any

VPN-1/Firewall-1 Policy Editor courtesy of Check Point Software Technologies Ltd.
Figure 5-4 Check Point VPN-1/Firewall-1 Policy Editor

Policy Management

- Policies must be managed as they constantly change
- To remain viable, security policies must have:
    - Individual responsible for the policy (policy administrator)
    - A schedule of reviews
    - Method for making recommendations for reviews
    - Specific 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
- More detailed version of security framework (outline of overall information security strategy for organization)
- Should specify tasks to be accomplished and the order in which they are to be realized
- Should also serve as scalable, upgradeable, and comprehensive plan for information security needs for coming years

The ISO 27000 Series

- One of the most widely referenced and often discussed security models
- 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 common basis for developing organizational security

Table 5-4 The ISO/IEC 27001: 2005 Plan-Do-Check-Act Cycle[14]

Plan	
1	Define the scope of the ISMS
2	Define an ISMS policy
3	Define the approach to risk assessment
4	Identify the risks
5	Assess the risks
6	Identify and evaluate options for the treatment of risk
7	Select control objectives and controls
8	Prepare a statement of applicability (SOA)

Table 5-4 (continued)

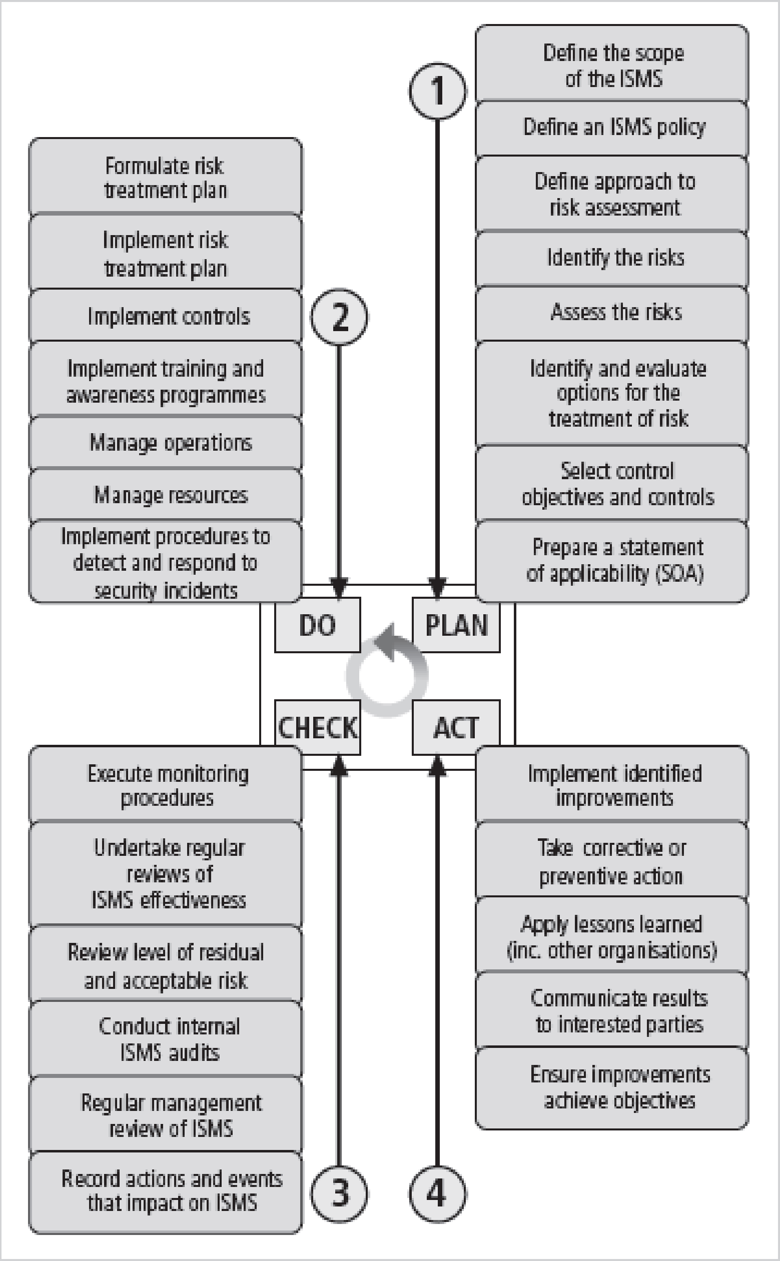
Do	
9	Formulate a risk treatment plan
10	Implement the risk treatment plan
11	Implement controls
12	Implement training and awareness programs
13	Manage operations
14	Manage resources
15	Implement procedures to detect and respond to security incidents

Table 5-4 (continued)

Check	
15	Execute monitoring procedures
16	Undertake regular reviews of ISMS effectiveness
17	Review the level of residual and acceptable risk
18	Conduct internal ISMS audits
19	Undertake regular management review of the ISMS
20	Record actions and events that impact an ISMS

Table 5-4 (continued)

Act	
21	Implement identified improvements
22	Take corrective or preventive action
23	Apply lessons learned
24	Communicate results to interested parties
25	Ensure improvements achieve objectives


1
Define the scope of the ISMS
Define an ISMS policy
Define approach to risk assessment
Identify the risks
Assess the risks
Identify and evaluate options for the treatment of risk
Select control objectives and controls
Prepare a statement of applicability (SOA)
2
Formulate risk treatment plan
Implement risk treatment plan
Implement controls
Implement training and awareness programmes
Manage operations
Manage resources
Implement procedures to detect and respond to security incidents
DO
PLAN
CHECK
ACT
Execute monitoring procedures
Undertake regular reviews of ISMS effectiveness
Review level of residual and acceptable risk
Conduct internal ISMS audits
Regular management review of ISMS
Record actions and events that impact on ISMS
3
Implement identified improvements
Take corrective or preventive action
Apply lessons learned (inc. other organisations)
Communicate results to interested parties
Ensure improvements achieve objectives
4

Courtesy of Gamma Secure Systems

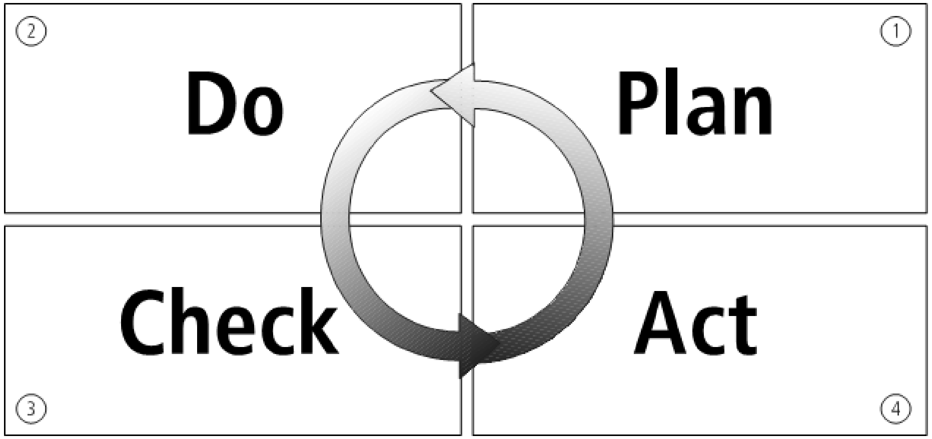
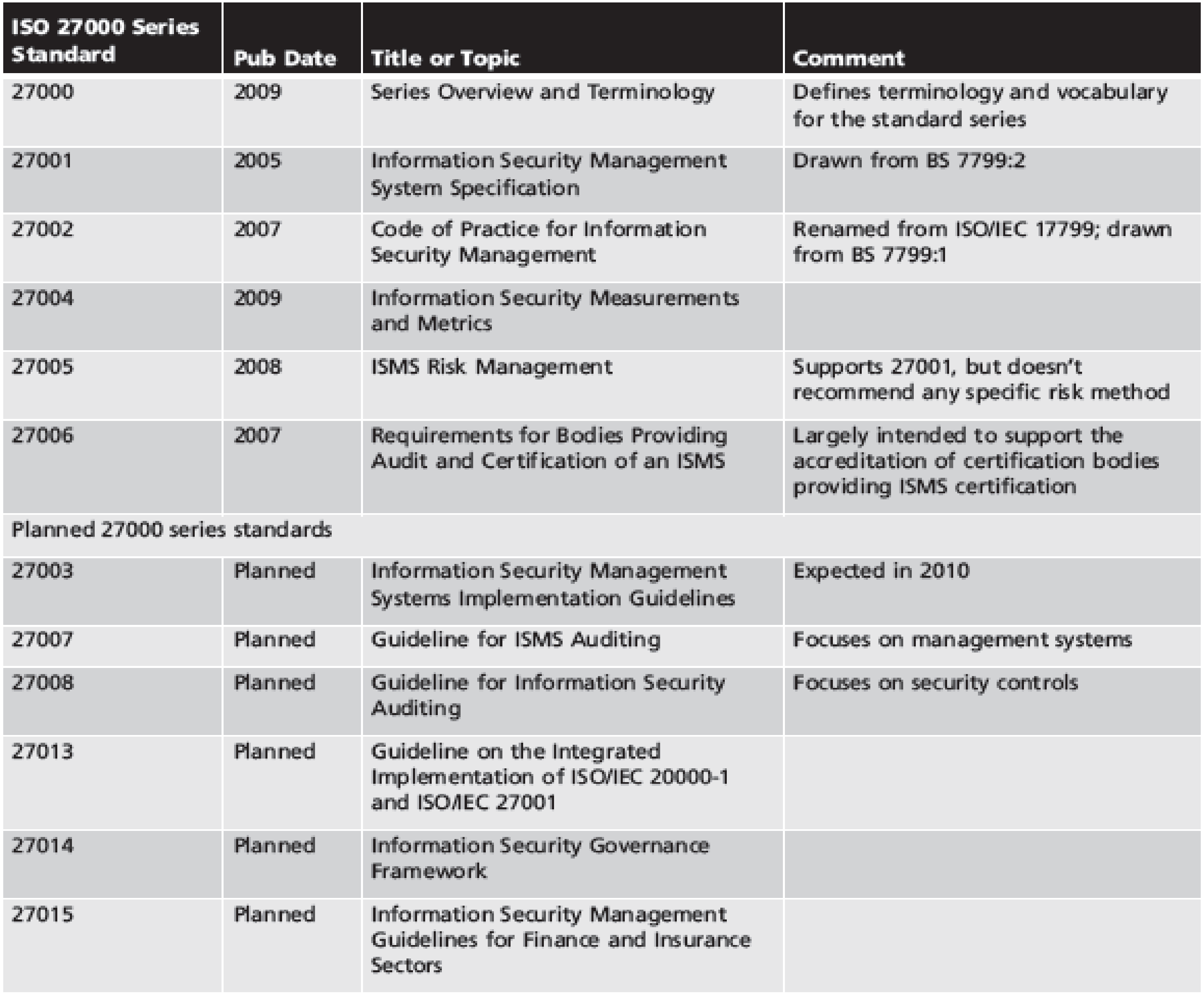


Figure 5-6 BS7799:2 Major Process Steps



ISO 27000 Series Standard	Pub Date	Title or Topic	Comment
27000	2009	Series Overview and Terminology	Defines terminology and vocabulary for the standard series
27001	2005	Information Security Management System Specification	Drawn from BS 7799:2
27002	2007	Code of Practice for Information Security Management	Renamed from ISO/IEC 17799; drawn from BS 7799:1
27004	2009	Information Security Measurements and Metrics	
27005	2008	ISMS Risk Management	Supports 27001, but doesn't recommend any specific risk method
27006	2007	Requirements for Bodies Providing Audit and Certification of an ISMS	Largely intended to support the accreditation of certification bodies providing ISMS certification
Planned 27000 series standards			
27003	Planned	Information Security Management Systems Implementation Guidelines	Expected in 2010
27007	Planned	Guideline for ISMS Auditing	Focuses on management systems
27008	Planned	Guideline for Information Security Auditing	Focuses on security controls
27013	Planned	Guideline on the Integrated Implementation of ISO/IEC 20000-1 and ISO/IEC 27001	
27014	Planned	Information Security Governance Framework	
27015	Planned	Information Security Management Guidelines for Finance and Insurance Sectors	

Table 5-5 ISO 27000 Series Current and Planned Standards

NIST Security Models

- Documents available from Computer Security Resource Center of NIST
  - SP 800-12, *The Computer Security Handbook*
  - SP 800-14, *Generally Accepted Principles and Practices for Securing IT Systems*
  - SP 800-18, *The Guide for Developing Security Plans for IT Systems*
  - SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*
  - SP 800-30, *Risk Management Guide for Information Technology Systems*

Principles and Practices for Securing IT Systems

1	Establish a sound security policy as the foundation for design
2	Treat security as an integral part of the overall system design
3	Clearly delineate the physical and logical security boundaries governed by associated security policies
4	Reduce risk to an acceptable level.
5	Assume that external systems are insecure.
6	Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
7	Implement layered security (ensure no single point of vulnerability).
8	Implement tailored system security measures to meet organizational security goals.
9	Strive for simplicity.
10	Design and operate an IT system to limit vulnerability and to be resilient in response.
11	Minimize the system elements to be trusted

Principles and Practices for Securing IT Systems

12	Implement security through a combination of measures distributed physically and logically
13	Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
14	Limit or contain vulnerabilities.
15	Formulate security measures to address multiple overlapping information domains.
16	Isolate public access systems from mission critical resources (e.g., data, processes, etc.)
17	Use boundary mechanisms to separate computing systems and network infrastructures.
18	Where possible, base security on open standards for portability and interoperability.
19	Use common language in developing security requirements.
20	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
21	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.

Principles and Practices for Securing IT Systems

22	Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
23	Use unique identities to ensure accountability.
24	Implement least privilege.
25	Do not implement unnecessary security mechanisms.
26	Protect information while being processed, in transit, and in storage.
27	Strive for operational ease of use.
28	Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
29	Consider custom products to achieve adequate security.
30	Ensure proper security in the shutdown or disposal of a system.
31	Protect against all likely classes of “attacks.”
32	Identify and prevent common errors and vulnerabilities.
33	Ensure that developers are trained in how to develop secure software

IETF Security Architecture

- Security Area Working Group acts as advisory board for protocols and areas developed and promoted by the Internet Society
- RFC 2196: Site Security Handbook covers five basic areas of security with detailed discussions on development and implementation

Baselining and Best Business Practices

- Baselining and best practices are solid methods for collecting security practices, but provide less detail than a complete methodology
- Possible to gain information by baselining and using best practices and thus work backwards to an effective design
- The Federal Agency Security Practices (FASP) site (http://csrc.nist.gov/groups/SMA/fasp) is designed to provide best practices for public agencies and is adapted easily to private institutions

Design of Security Architecture

- Spheres of security: foundation of the security framework
- Levels of controls
  - Management controls cover security processes designed by strategic planners and performed by security administration
  - Operational controls deal with operational functionality of security in organization
  - Technical controls address tactical and technical implementations related to designing and implementing security in organization

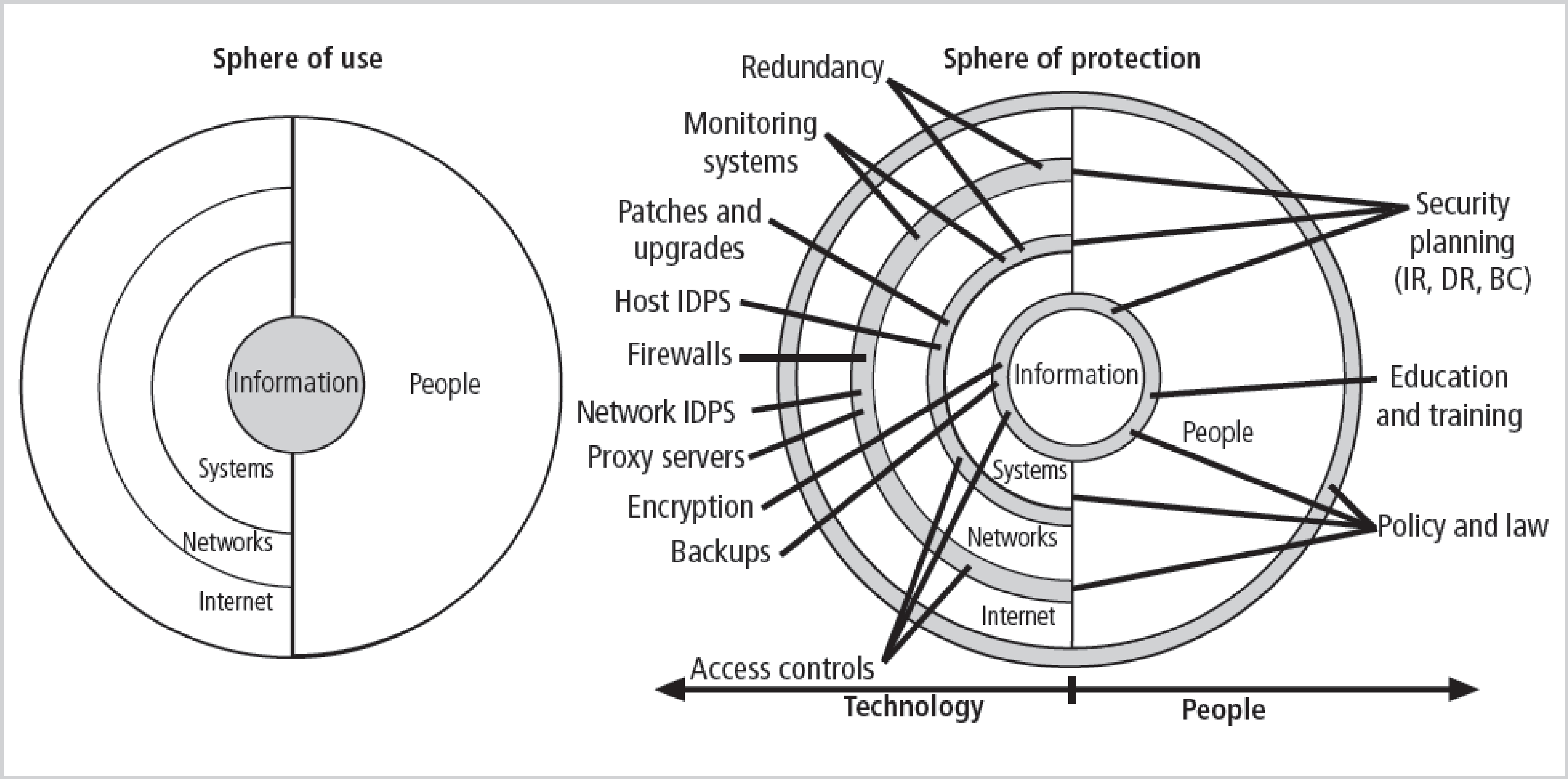


Figure 5-8 Spheres of Security

Design of Security Architecture (cont'd.)

- Defense in depth
  - Implementation of security in layers
  - Requires that organization establish sufficient security controls and safeguards so that an intruder faces multiple layers of controls
- Security perimeter
  - Point at which an organization's security protection ends and outside world begins
  - Does not apply to internal attacks from employee threats or on-site physical threats

Design of Security Architecture (cont'd.)

- Firewall: device that selectively discriminates against information flowing in or out of organization
- DMZs: no-man's land between inside and outside networks where some place Web servers
- Proxy servers: performs actions on behalf of another system
- Intrusion detection systems (IDSs): in effort to detect unauthorized activity within inner network, or on individual machines, organization may wish to implement an IDS

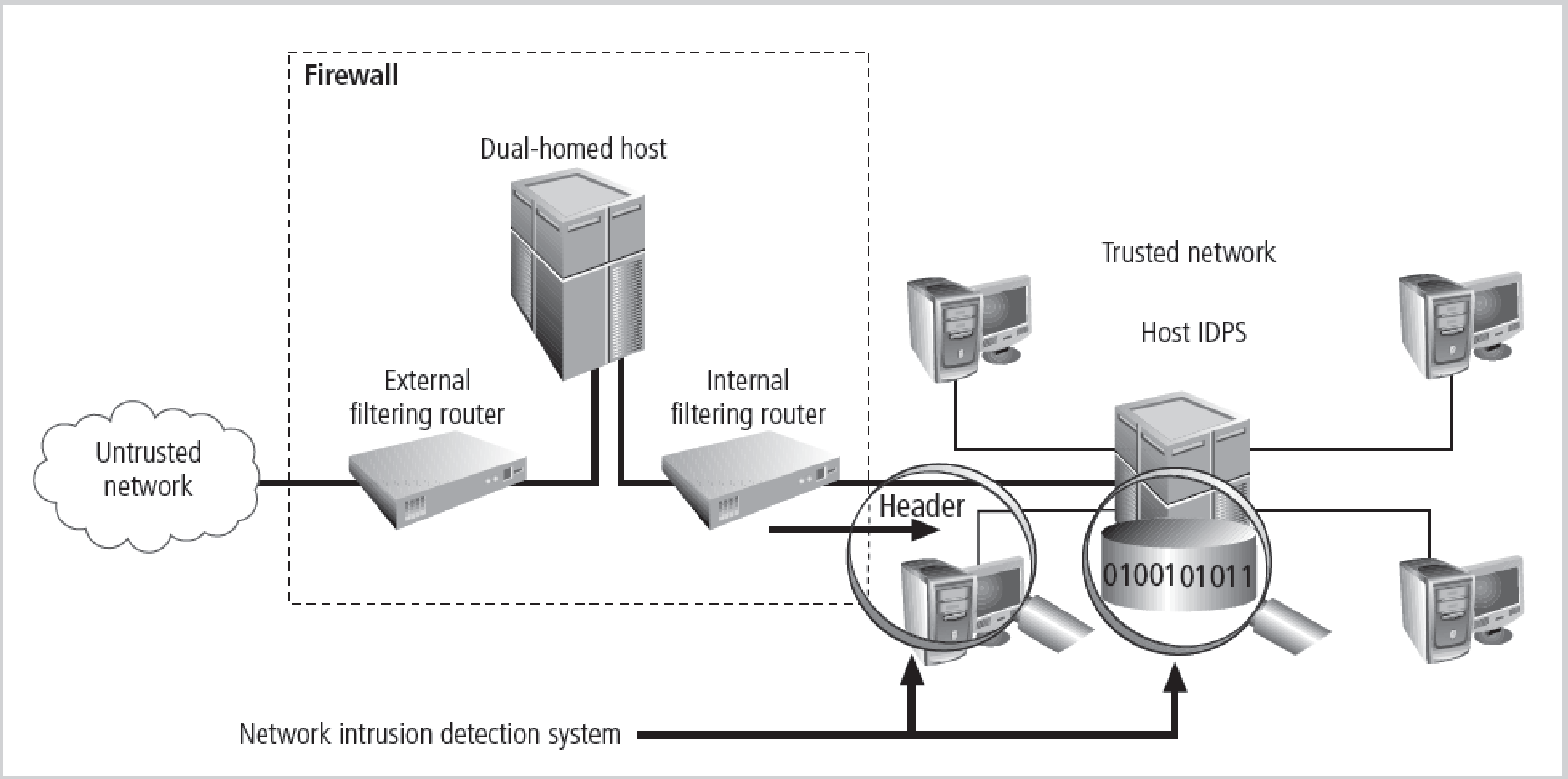

Firewall
Dual-homed host
Trusted network
Host IDPS
External filtering router
Internal filtering router
Untrusted network
Header
0100101011
Network intrusion detection system

Figure 5-9 Defense in Depth

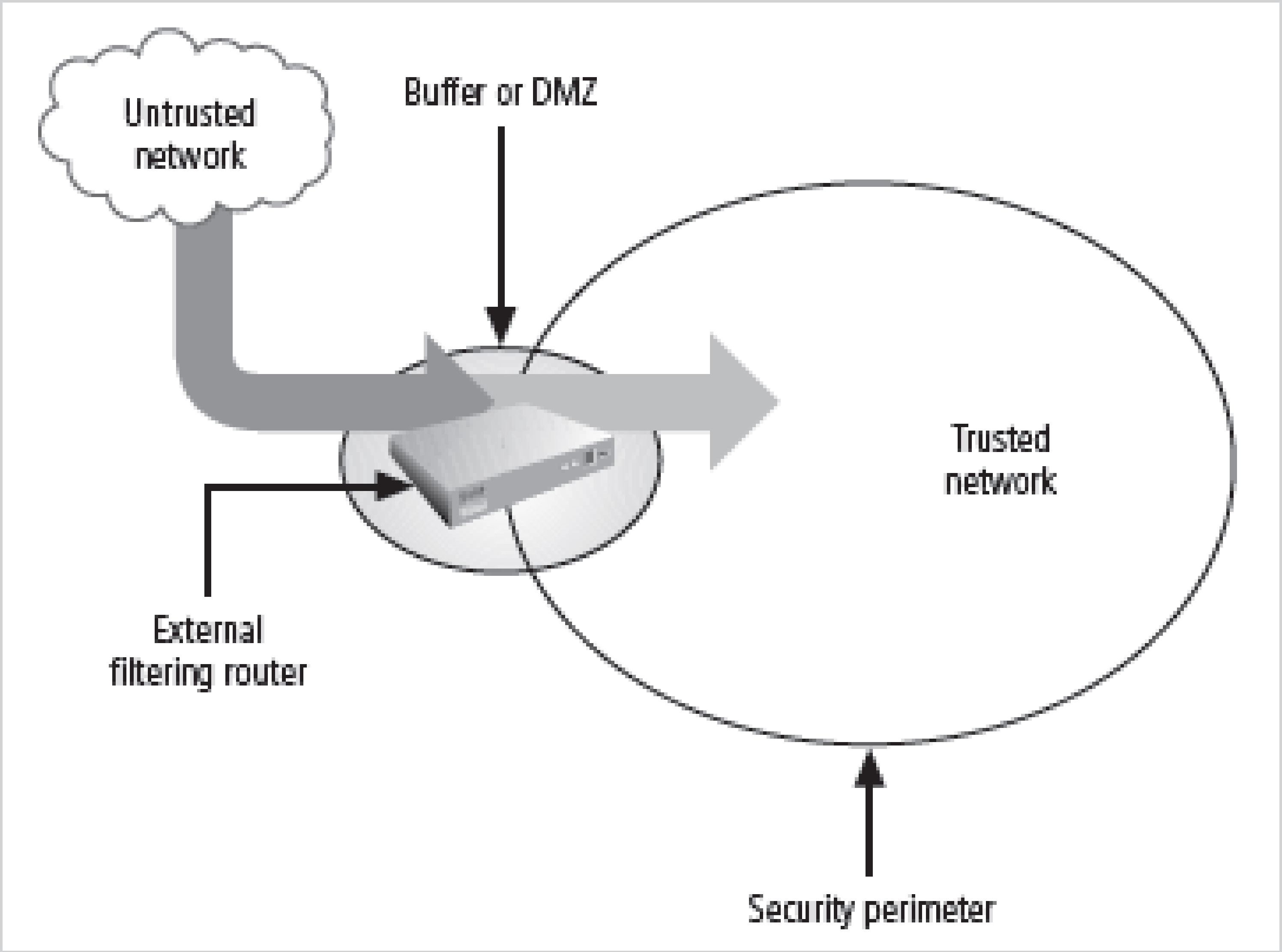


Figure 5-10 Security Perimeters

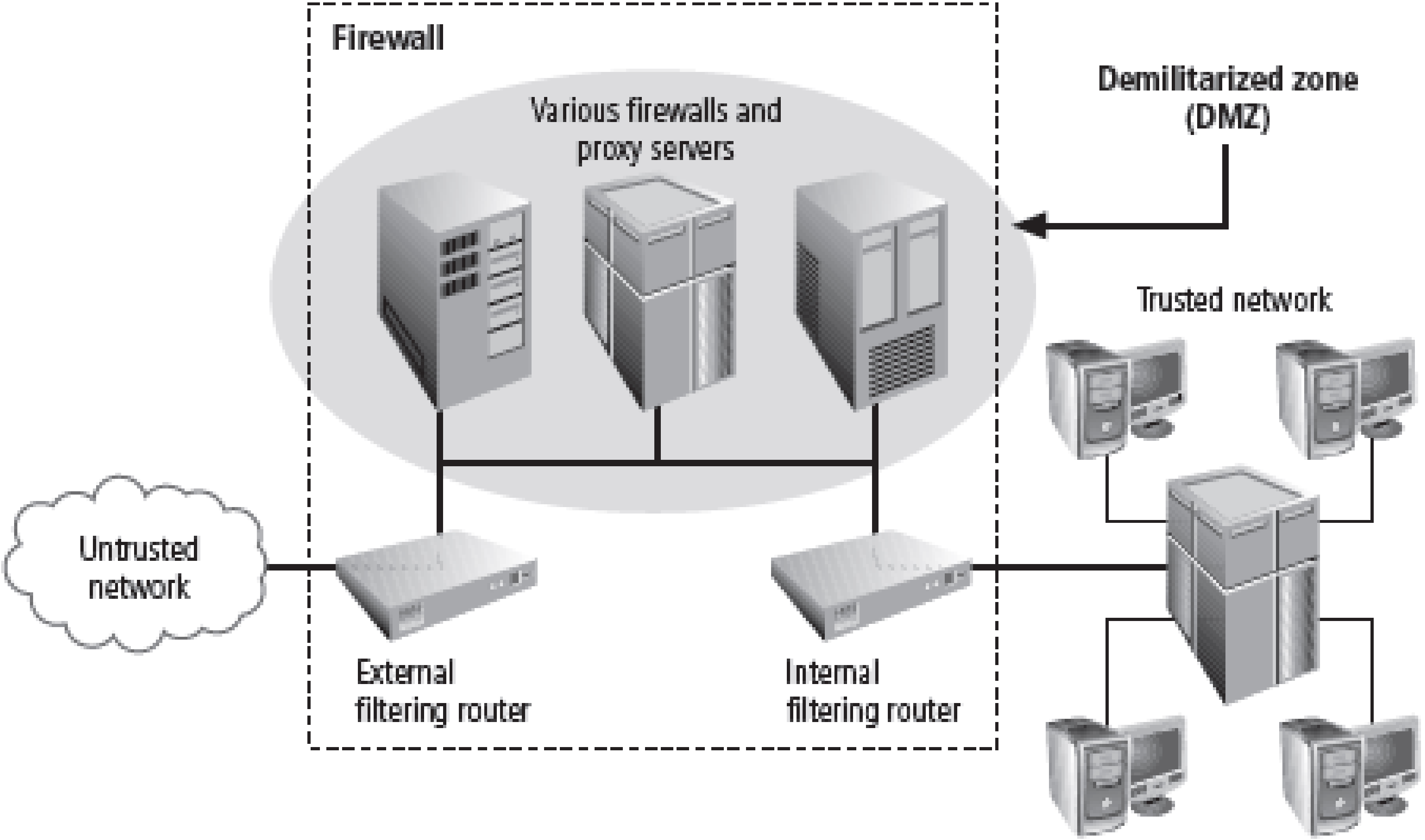

Firewall
Various firewalls and proxy servers
Demilitarized zone (DMZ)
Trusted network
Untrusted network
External filtering router
Internal filtering router

Figure 5-11 Firewalls, Proxy Servers, and DMZs

Security Education, Training and Awareness Program

- As soon as general security policy exists, policies to implement security education, training, and awareness (SETA) program should follow
- SETA is a control measure designed to reduce accidental security breaches
- Security education and training builds on the general knowledge the employees must possess to do their jobs, familiarizing them with the way to do their jobs securely
- The SETA program consists of: security education; security training; and security awareness

Security Education

- Everyone in an organization needs to be trained and aware of information security; not every member needs formal degree or certificate in information security
- When formal education for individuals in security is needed, an employee can identify curriculum available from local institutions of higher learning or continuing education
- A number of universities have formal coursework in information security

Security Training

- Involves providing members of organization with detailed information and hands-on instruction designed 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 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 begin to "tune out" and risk of employee accidents and failures increases

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, is closely associated with BCP
  - BCP occurs concurrently with DRP when damage is major or long term, requiring more than simple restoration of information and information resources

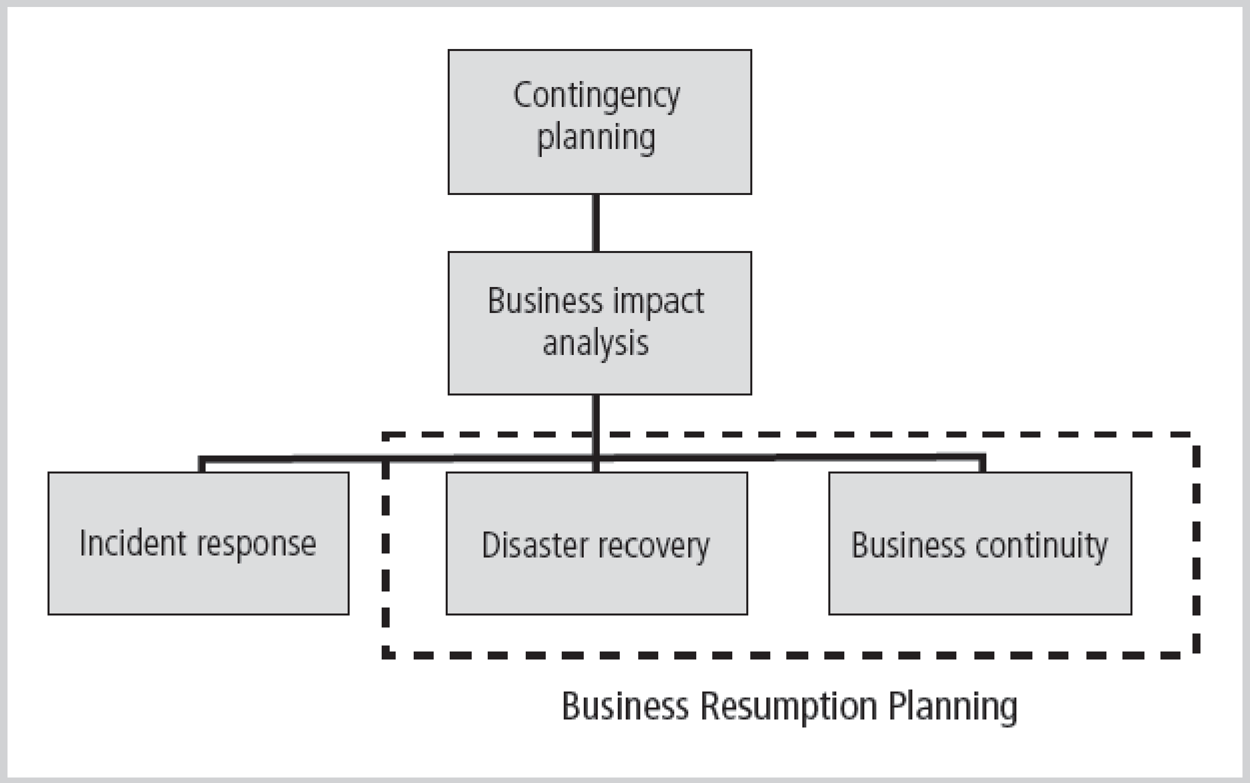


Figure 5-14 Components of Contingency Planning

Continuity Strategies (cont'd.)

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

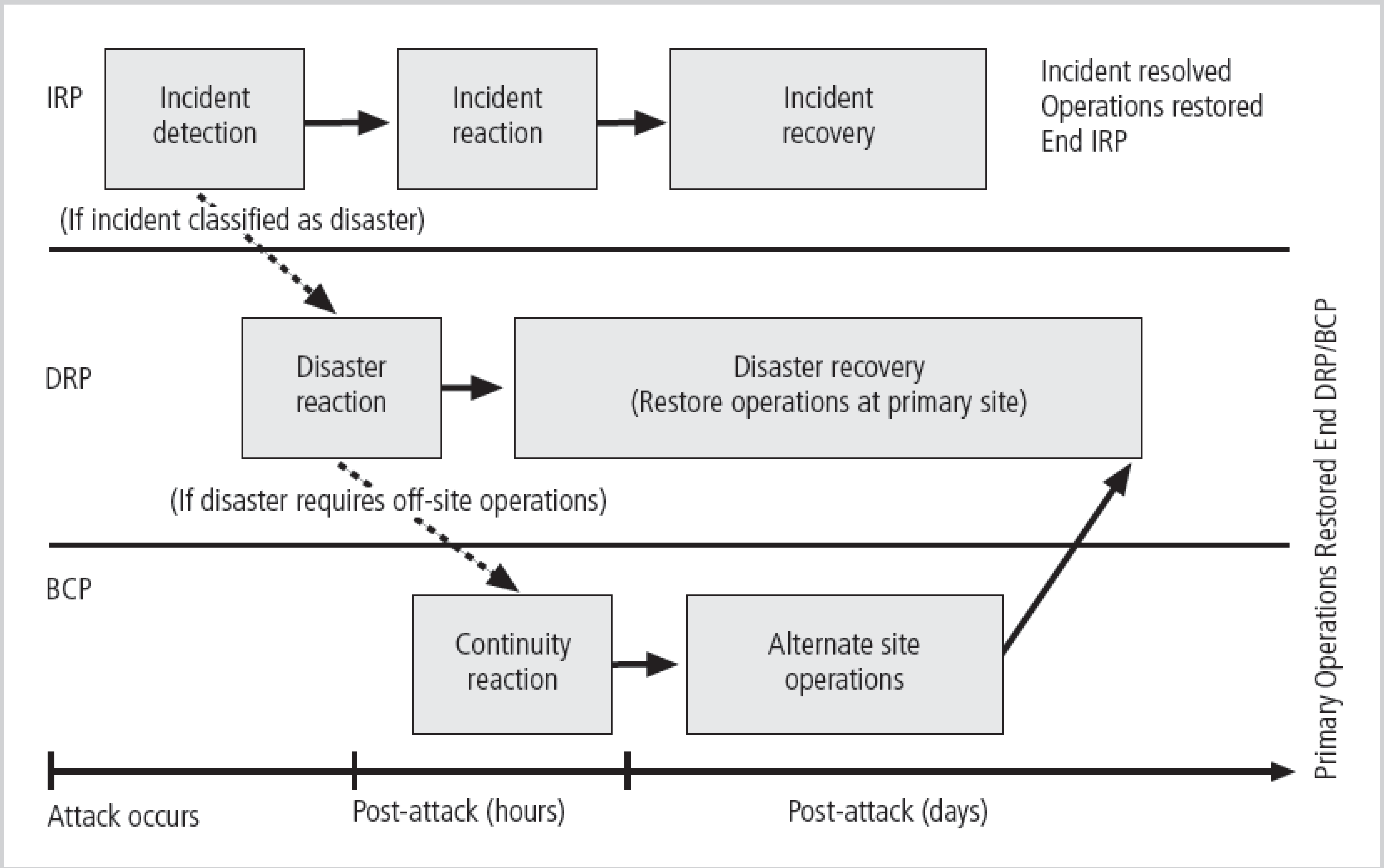


Figure 5-15 Contingency Planning Timeline

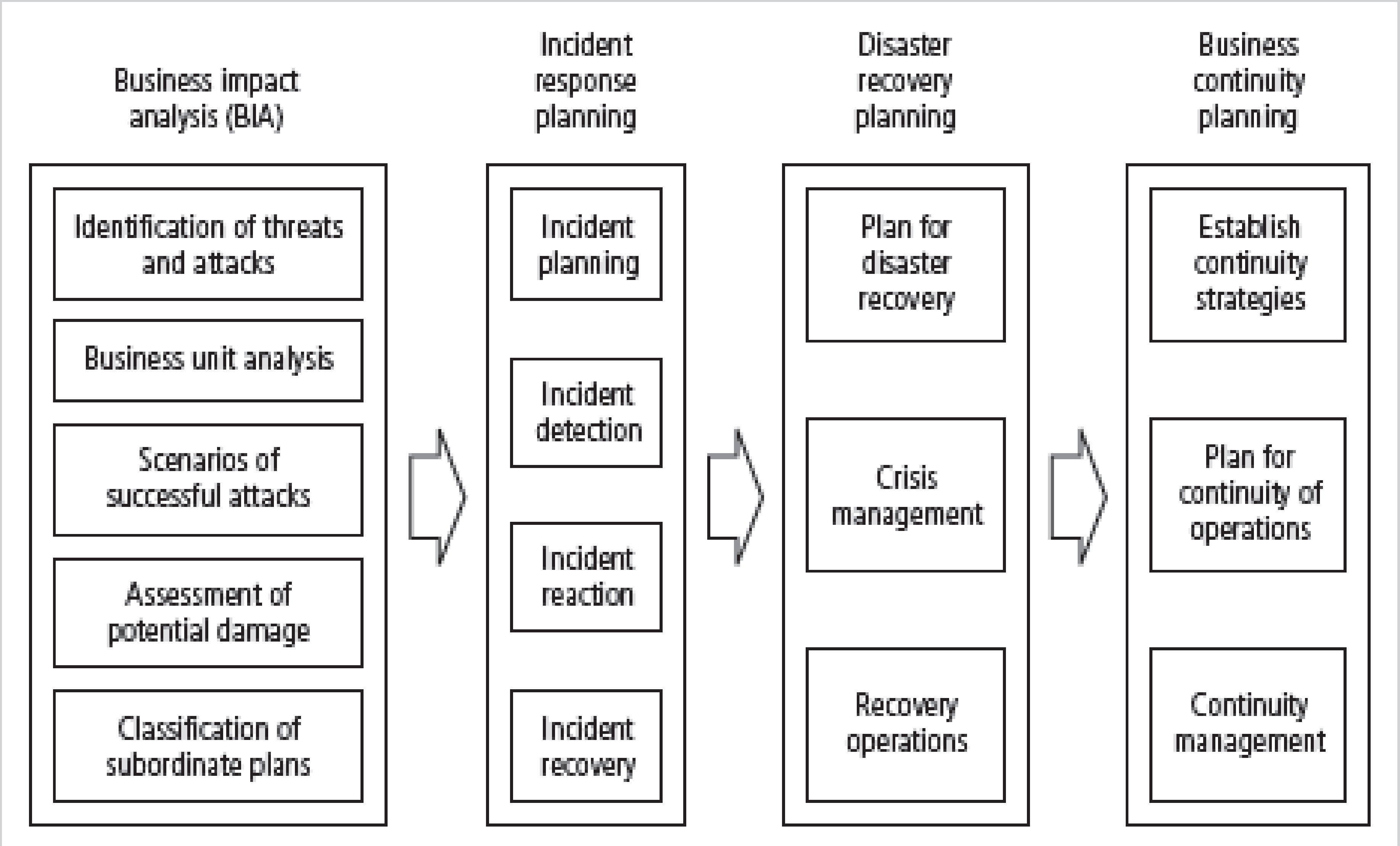

Business impact analysis (BIA)
Identification of threats and attacks
Business unit analysis
Scenarios of successful attacks
Assessment of potential damage
Classification of subordinate plans
Incident response planning
Incident planning
Incident detection
Incident reaction
Incident recovery
Disaster recovery planning
Plan for disaster recovery
Crisis management
Recovery operations
Business continuity planning
Establish continuity strategies
Plan for continuity of operations
Continuity management

Figure 5-16 Major Steps in Contingency Planning

Business Impact Analysis (BIA)

- Investigation and assessment of the impact that various attacks can have on the organization
- Assumes security controls have been bypassed, have failed, or have proven ineffective, and attack has succeeded
- Stages of BIA
  - Threat attack identification and prioritization
  - Business unit analysis
  - Attack success scenario development
  - Potential damage assessment
  - Subordinate plan classification

Incident Response Planning

- Incident response planning covers 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 Planning
  - First step in overall process of incident response planning
  - Predefined responses enable organization to react quickly and effectively to detected incident if:
    - Organization has IR team
    - Organization can detect incident
  - IR team consists of individuals needed to handle systems as incident takes place
  - Planners should develop guidelines for reacting to and recovering from incident

Incident Response Planning (cont'd.)

- Incident response plan
  - Format and content
  - Storage
  - Testing
- Incident detection
  - Most common occurrence is complaint about technology support, often delivered to help desk
  - Careful training needed to quickly identify and classify an incident
  - Once attack is properly identified, organization can respond

Incident Response Planning (cont'd.)

- Incident reaction
  - Consists of actions that guide organization to stop incident, mitigate the impact of incident, and provide information for recovery from incident
  - Actions that must occur quickly:
    - Notification of key personnel
    - Documentation of incident
- Incident containment strategies
  - First the areas affected must be determined
  - 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 retrieved, the next stage is recovery
  - 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, 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 acceptable 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
  - downside of current automated response systems may outweigh benefits

Disaster Recovery Planning

- Disaster recovery planning (DRP) is planning the preparation for and recovery from a disaster
- The contingency planning team must decide which actions constitute disasters and which constitute incidents
- When situations 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

- Outlines reestablishment of critical business operations during a disaster that impacts operations
- If disaster has rendered the business unusable for continued operations, 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
  - Dedicated recovery site options
    - Hot sites – fully operational sites
    - Warm sites – fully operational hardware but software may not be present
    - Cold sites – rudimentary services and facilities

Business Continuity Planning (cont'd.)

- Shared site options: time-share, service bureaus, and mutual agreements
- Time-share - A hot, warm, or cold site that is leased in conjunction with a business partner or sister organization
- Service Bureaus – An agency that provides a service for a fee.
- Mutual agreement - A contract between two or more organizations that specifies how each will assist the other in the event of a disaster.

Business Continuity Planning (cont'd.)

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

Crisis Management

- Actions taken during and after a disaster that focus on people involved and address viability of business
- 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 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

Model for a Consolidated Contingency Plan

- Single document set approach supports concise planning and encourages smaller organizations to develop, test, and use IR and DR plans
- Model is based on analyses of disaster recovery and incident response plans of dozens of organizations
- The planning document

Model for a Consolidated Contingency Plan (cont'd.)

- Six steps in contingency planning process
  - Identifying mission- or business-critical functions
  - Identifying resources that support critical functions
  - Anticipating potential contingencies or disasters
  - Selecting contingency planning strategies
  - Implementing contingency strategies
  - Testing and revising strategy

Summary

- 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

Summary (cont’d.)

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