

TEL2813/IS2621

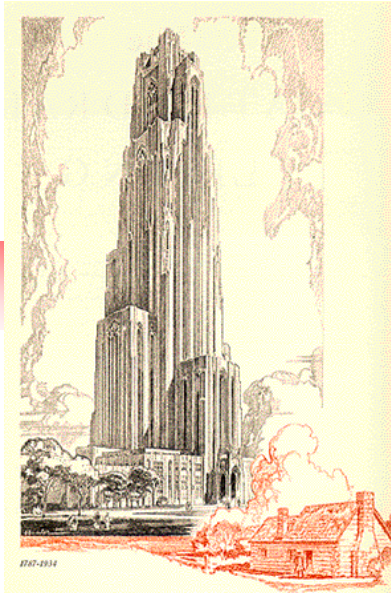
Security Management

James Joshi

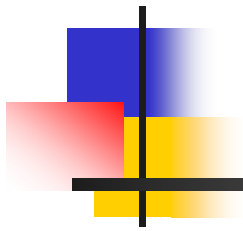
Associate Professor

Lecture 2

Jan 15, 2015



Contingency Planning
InfoSec Policy, & Program



Contingency Planning

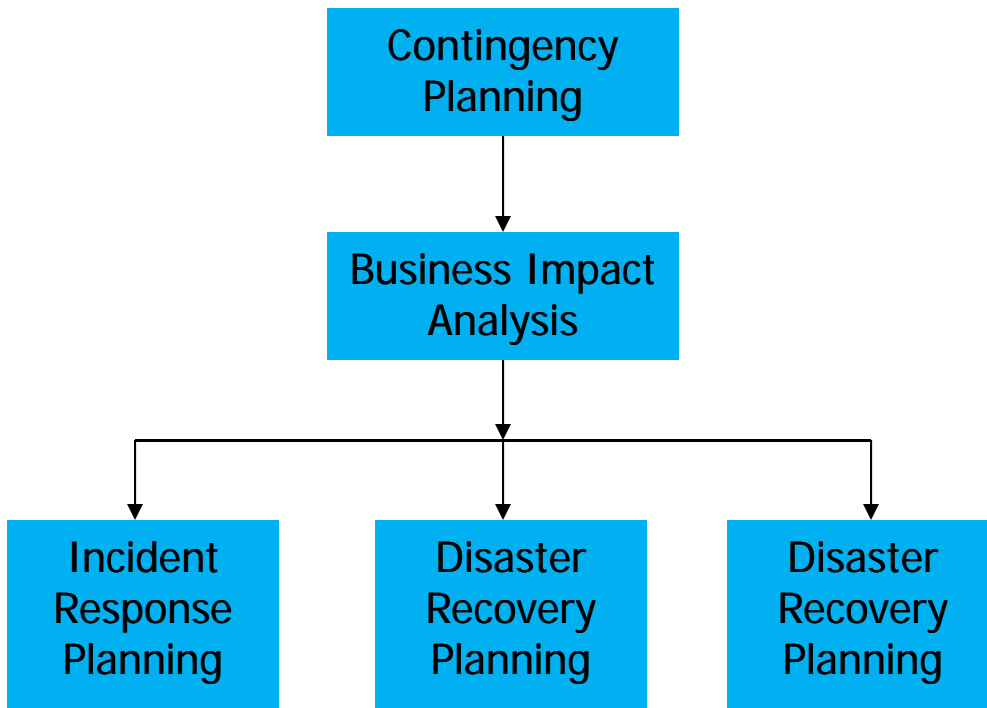


What Is Contingency Planning?

- Contingency planning (CP)
 - Overall planning for unexpected events
 - to prepare for, detect, react to, and recover from undesirable events
- Main goal:
 - restoration to normal modes of operation with minimum cost and disruption to normal business activities after an unexpected event



CP Components



- **Business Impact Analysis (BIA)**
 - focuses on the understanding impact
- **Incident response (IRP)**
 - focuses on immediate response
- **Disaster recovery (DRP)**
 - focuses on restoring operations at the primary site after disasters occur
- **Business continuity (BCP)**
 - facilitates establishment of operations at an alternate site



CP Components (Continued)

- Contingency planners should:
 - Identify the mission- or business-critical functions
 - Identify resources that support critical functions
 - Anticipate potential contingencies or disasters
 - Select contingency planning strategies
 - Implement selected strategy
 - Test and revise contingency plans
- Teams involved in contingency planning/operations:
 - CP team (Champion, Project Manager, Team members – CPMT)
 - Incident recovery (IR) team
 - Disaster recovery (DR) team
 - Business continuity plan (BC) team



Incident Response Plan

- **IRP:**
 - Detailed set of processes and procedures that **anticipate**, **detect**, and **mitigate** the impact of an unexpected event that might compromise information resources/assets
- **Incident response (IR):**
 - Set of procedures that commence when an incident is detected
 - Is a **reactive** measure, not a **preventive** one



Incident-handling procedures

- IR Planning team drafts a set of procedures,
 - For **Before the Incident**
 - Details of data backup schedules
 - Disaster recovery preparation
 - Training schedules
 - Testing plans
 - Copies of service agreements
 - Business continuity plans
 - For **During the Incident**
 - These procedures are grouped and assigned to various roles
 - Planning committee drafts a set of function-specific procedures
 - For **After the Incident**
 - planners develop and document the procedures that must be performed immediately after the incident has ceased
 - Separate functional areas may develop different procedures

Before an Attack

Users

1. Don't put suspicious diskettes in your system.
2. Check your system before booting.
3. Don't download free games or use the Internet on your system without authorization from the Information Services department.
4. Don't open attachments in unsolicited e-mail. Make sure all attachments are from a trusted source or a third party by confirming the origin in the e-mail header.
5. Don't forward messages that ask you to forward them to warn others of a virus or threat.

Technology Services

1. Ensure virus protection software is properly configured, and update definitions regularly.
2. Automate whenever possible. Provide awareness and training to users on proper use of the e-mail and Internet, and antivirus software.

After an Attack

Users

1. Scan your computer thoroughly for any additional viruses.
2. Review e-mail (TITLES ONLY, DO NOT REOPEN attachments) for suspicious activity.
3. Write down everything you were doing before you detected the virus.
4. Verify that your antivirus software definitions are up-to-date.

Technology Services

1. Conduct an incident recovery investigation.
2. Interview all users detecting the virus.
3. Verify that all systems antivirus definitions are up-to-date.
4. Reconnect quarantined users to the network.
5. Brief all infected users on proper use of the Internet and e-mail.
6. File the incident recovery investigation report. Notify all users that this particular strain of virus has been detected, and that they should update their antivirus software and definitions.

During an Attack

Users

1. If your antivirus software detects an attack, it will delete the virus or quarantine the file that carries it. Record any messages that your antivirus software displays and notify Technology Services immediately.
2. If your computer begins behaving unusually or you determine that you have contracted a virus through other means, turn your computer off immediately, by pulling the plug. Notify Technology Services immediately.

Technology Services

1. If users begin reporting virus attacks, record the information provided by the users.
2. Temporarily disconnect those users from the network at the switch.
3. Begin scanning all active systems for that strain of virus.
4. Deploy a response team to inspect the users' system.

FIGURE 3-2 Incident Response Planning



Incident Detection

- Challenge
 - determining whether an event is routine system use or an actual incident
- Incident classification
 - process of examining a possible incident and determining whether or not it constitutes an actual incident
- Ways to track and detect incident candidates
 - Initial reports from end users, IDS, virus detection software, and systems administrators
- Careful training is needed to allow everyone to relay vital information to the IR team



Incident Indicators

- Possible Indicators

- Presence of unfamiliar files
- Presence or execution of unknown programs or processes
- Unusual consumption of computing resources
- Unusual system crashes

- Probable Indicators

- Activities at unexpected times
- Presence of new accounts
- Reported attacks
- Notification from IDS

- Definite Indicators

- Use of dormant accounts
- Changes to logs
- Presence of hacker tools
- Notifications by partner or peer
- Notification by hacker

- Actual occurrences

- Loss of availability
- Loss of integrity
- Loss of confidentiality
- Violation of policy
- Violation of law



Incident Response

- In the incident response phase,
 - Action steps taken by the IR team and others must occur **quickly** and **concurrently** --- Proper Coordination/Collaboration
- Notify right people ASAP,
 - Alert roster: *sequential, hierarchical*
 - Alert message:
 - scripted description of incident
 - Other key personnel:
 - must also be notified only after incident has been confirmed,
 - before media or other external sources learn of it
- **DOCUMENT**: Record the **who, what, when, where, why** and **how** of each action taken while the incident is occurring
 - Legal side, due care



Incident Containment Strategies

- IR team can **stop** the incident and attempt to **recover** control by means of several strategies:
 - Disconnect affected communication circuits
 - Dynamically apply filtering rules to limit certain types of network access
 - Disable compromised user accounts
 - Reconfigure firewalls to block problem traffic
 - Temporarily disable compromised process/service
 - Take down conduit application or server
 - Stop all computers and network devices

Control incident escalation !!



Initiating Incident Recovery

- Incident recovery
 - Done after the incident has been contained, and system control regained
 - Inform Human resources
 - Assess full extent of damage in order to determine what must be done to restore systems – and use IRP to carry out IR operations
- Incident damage assessment
 - Determine the scope of the breach of confidentiality, integrity, and availability of information assets
 - Document damage and Preserve evidence
 - In case the incident is part of a crime or results in a civil action



Recovery Process

- Once the extent of the damage has been determined, the recovery process begins:
 - Identify and resolve **vulnerabilities** that allowed the incident
 - Address, install, and replace/upgrade **safeguards** that failed to stop or limit the incident, or were missing
 - Evaluate monitoring capabilities to improve **detection and reporting** methods, or install new **monitoring capabilities**
 - Restore data from backups as needed – need a **backup strategy!**
 - Restore services and processes in use
 - Continuously monitor system - **maintain vigilance**
 - Restore the confidence of the members of the organization's communities of interest



After Action Review

- Before returning to routine duties,
 - the IR team must conduct an after-action review (AAR):
 - detailed examination of events that occurred
- All team members:
 - Review their actions during the incident
 - Identify areas where the IR plan worked, didn't work, or should improve



Law Enforcement Involvement

- When incident violates civil or criminal law,
 - Make sure to notify proper authorities
 - Selecting appropriate law enforcement agency
 - Federal, State, or Local (depending on crime)
- Involvement of law enforcement (advantages and disadvantages):
 - Usually much better at processing evidence, obtaining statements from witnesses, and building legal cases
 - Does the org have Computer Forensics capability?
 - Involvement can result in **loss of control of chain** of events following an incident
 - What is the legal obligation – to report or not?



Disaster Recovery

- **DRP**

- Preparation for and recovery from a disaster, whether natural or man made

- In general, an incident is a disaster when:

- organization is *unable* to **contain or control** the impact
 - OR
 - level of damage or destruction from incident is so *severe*, the organization is unable to quickly recover

- **Key role of DRP:**

- defining how to reestablish operations at location where organization is usually located



Disaster Classifications

- A DRP can classify disasters in a number of ways
 - Most common:
 - Separate natural disasters from man-made disasters
 - Another way: by speed of development
 - Rapid onset disasters
 - Earthquake, floods, storms, tornadoes
 - Slow onset disasters
 - Droughts, famines, env degradation, deforestation, pest infestation



Planning for Disaster

- Categorize threat level of potential disasters
 - Uses Scenario development and impact analysis
- DRP must be tested regularly
- Key points in the DRP:
 - Clear delegation of roles and responsibilities
 - Execution of alert roster and notification of key personnel
 - Clear establishment of priorities
 - Documentation of the disaster
 - Action steps to mitigate the impact
 - Alternative implementations for various systems components



Crisis Management

- DRP should refer to a CM process
 - Set of focused steps taken during and after a disaster that deal primarily with people involved
- Crisis management team manages event:
 - Supporting personnel and their loved ones during crisis
 - Determining event's impact on normal business operations, when necessary, making a disaster declaration
 - Keeping public informed about event
 - Communicating with outside parties
- Two key tasks of crisis management team:
 - Verifying personnel status
 - Activating alert roster



Responding to the Disaster

- Actual events often **outstrip** even best of plans
- To be prepared, DRP should be **flexible**
- If physical facilities are intact, begin restoration there
- If organization's facilities are **unusable**, take alternative actions
- When disaster threatens organization at the **primary site**, DRP becomes BCP



Business Continuity Planning (BCP)

- Ensures **critical business functions** can continue in a disaster
- Most properly managed by **CEO** of organization
- Activated and executed concurrently with the DRP when needed
- Reestablishes **critical functions at alternate site** (DRP focuses on reestablishment at primary site)
- Relies on identification of critical business functions and the resources to support them



Continuity Strategies

- Several continuity strategies for business continuity
 - Determining factor is usually **cost**

- Three exclusive-use options:

- Hot sites

- Fully configured computer facility with all services
- Where 24/7 support is needed

- Warm sites

- Like hot site, but software applications not kept fully prepared

- Cold sites

- Only rudimentary services and facilities kept in readin

Cost
↓

Site	Cost	Hardware Equipment	Telecommunications	Setup Time	Location
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed
Hot Site	Medium/High	Full	Full	Short	Fixed



Shared Use Options

- Timeshares
 - Like an exclusive use site but leased – lower cost
 - Disadvantages
 - More than one may need it simultaneously
 - Data and info asset from many different organizations
- Service Bureaus
 - Agency that provides physical facilities/data storage – for a fee
 - Renegotiation periodically
- Mutual Agreements
 - Contract between two organizations to assist (or units within)
- Specialized alternatives/variations:
 - Rolling mobile site
 - Mirrored
 - Externally stored resources



Off-Site Disaster Data Storage

- To get any BCP site running quickly,
 - organization must be able to move data to new site
- Options include:
 - **Electronic vaulting:**
 - bulk batch-transfer of data to an off-site facility
 - Leased lines may be used
 - **Remote Journaling:**
 - transfer of **live transactions** to an off-site facility (not focused on data archives)
 - **Database shadowing**
 - storage of duplicate online transaction data and duplicate databases on redundant server
 - Combines electronic vaulting and remote journaling

Contingency Plan Implementation Timeline

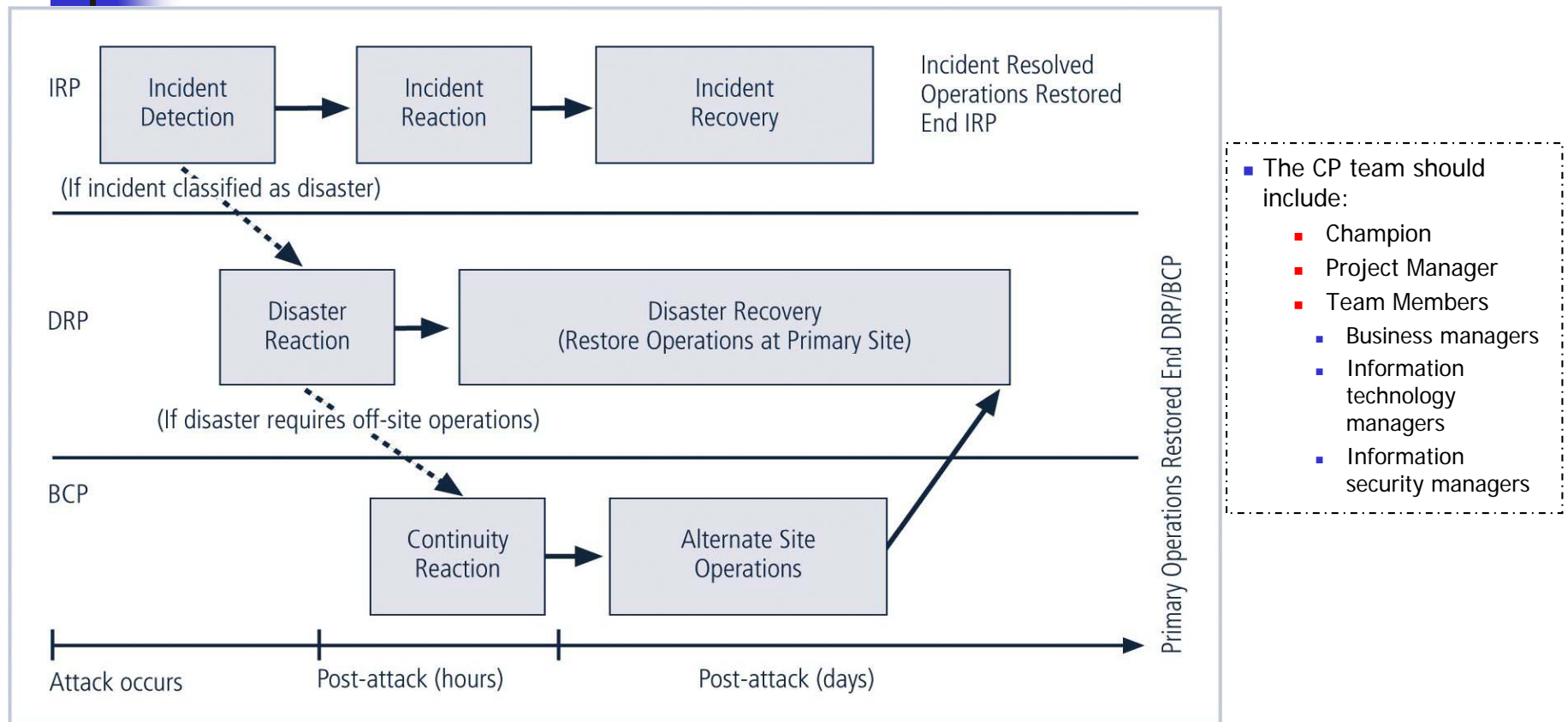


FIGURE 3-5 Contingency Plan Implementation Timeline

Major Tasks in Contingency Planning (for CP team)

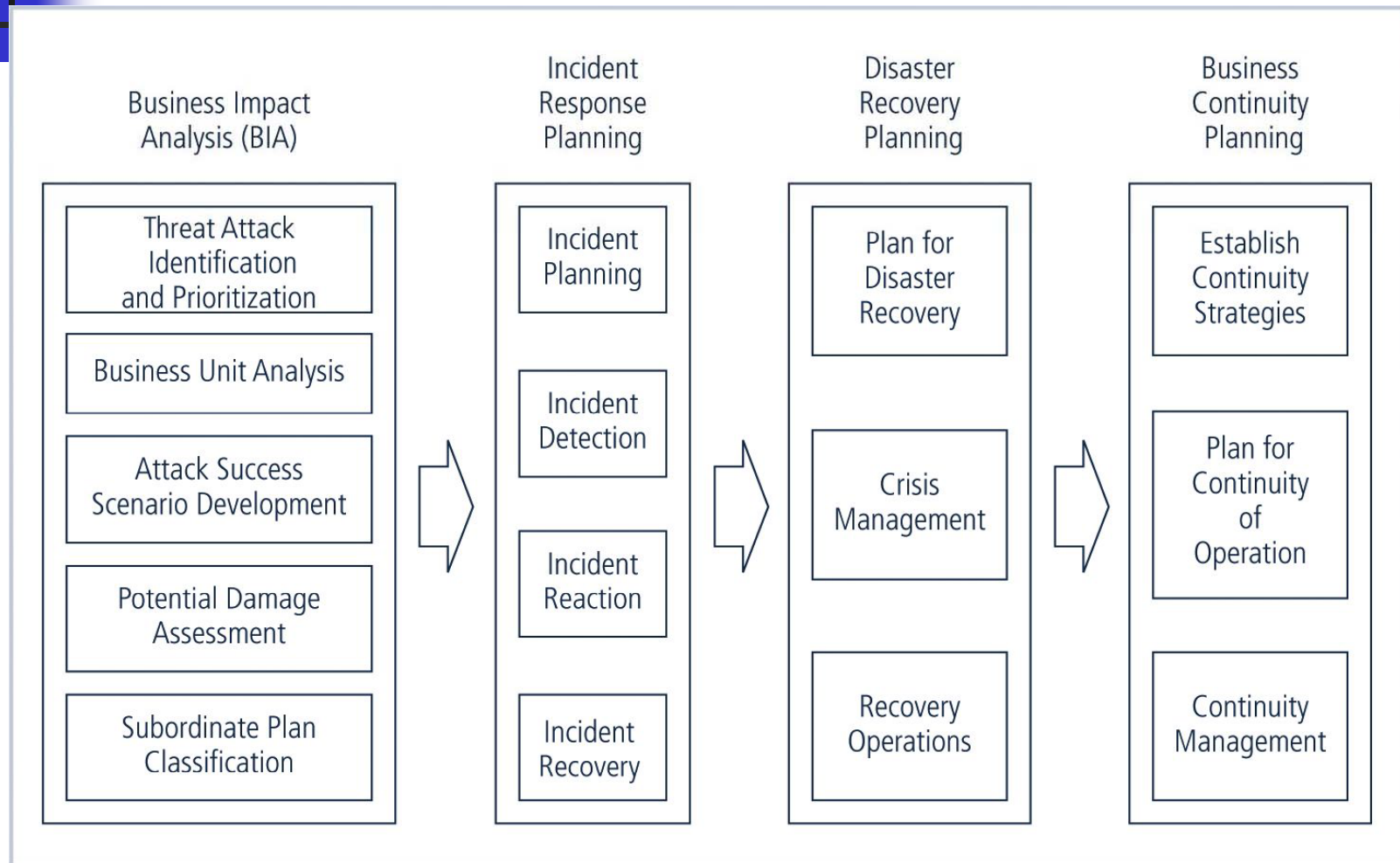


FIGURE 3-6 Major Tasks in Contingency Planning



Business Impact Analysis (BIA)

- BIA
 - Provides information about systems/threats and detailed scenarios for each potential attack
 - Not risk management
 - RM focuses on identifying threats, vulnerabilities, and attacks to determine controls
 - BIA assumes controls have been bypassed or are ineffective and attack was successful
- CP team conducts BIA in the following stages:
 - Threat attack identification
 - Business unit analysis
 - Attack success scenarios
 - Potential damage assessment
 - Subordinate plan classification



Business Impact Analysis

- Threat/Attack Identification and Prioritization
 - Add the attack profile to identified and prioritized threats
 - risk management process will have identified and prioritized threats
 - Attack profile:
 - detailed description of activities that occur during an attack
 - (handout page)
- Business Unit Analysis
 - Analysis and prioritization of business functions within the organization
 - Each unit should be considered separately



BUA, ASSD, PDA

- **Attack Success Scenario Development**
 - Create a series of scenarios on each functional area
 - Attack profiles should include scenarios attack including:
 - Methodology
 - Indicators
 - Broad consequences
 - More details are added including
 - alternate outcomes—best, worst, and most likely
- **Potential Damage Assessment**
 - Estimate the cost of the best, worst, and most likely outcomes
 - Identify what must be done to recover from each possible case
- **Subordinate Plan Classification**
 - Identify a related plan from among existing plans
 - Categorize attack scenario case as disastrous or not



Combined DRP and BCP

- DRP and BCP are closely related,
 - Most organizations prepare them concurrently and
 - May combine them into a single document
 - Plan must support reestablishment of operations
 - Immediately at alternate site
 - Eventually back at primary site
- A single team can develop combined DRP/BRP,
 - but execution requires separate teams



Sample Disaster Recovery Plan

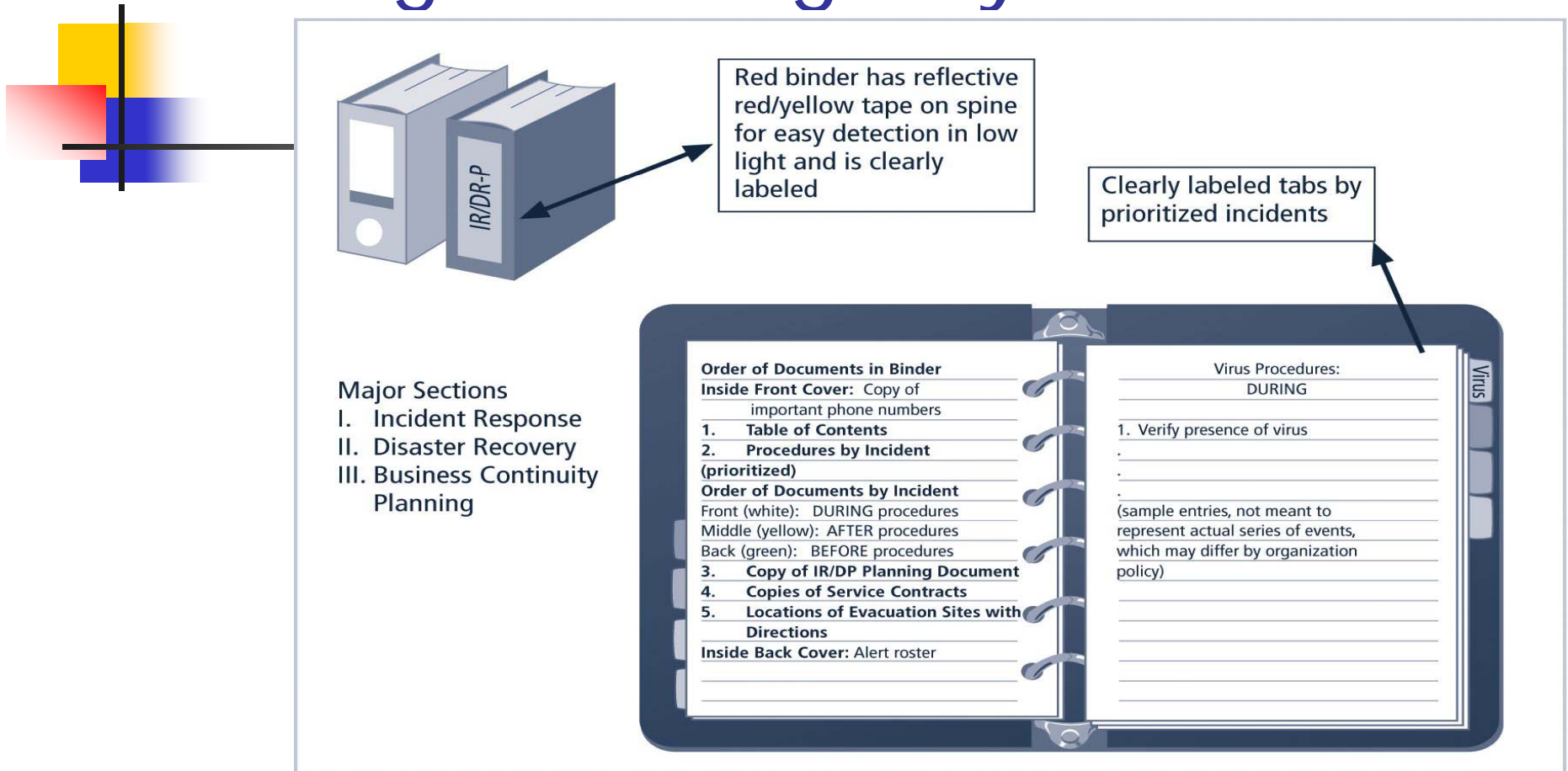
- Name of agency
- Date of completion or update of the plan and test date
- Agency staff to be called in the event of a disaster
- Emergency services to be called (if needed) in event of a disaster
- Locations of in-house emergency equipment and supplies
- Sources of off-site equipment and supplies
- Salvage Priority List
- Agency Disaster Recovery Procedures
- Follow-up Assessment



Testing Contingency Plans

- After testing process,
 - improvements can be made, and the resulting plan can be relied on in times of need
- There are five testing strategies that can be used to test contingency plans:
 - Desk Check
 - Structured walkthrough
 - Simulation
 - Parallel testing
 - Full interruption

A Single Contingency Plan Format



Continuous Process Improvement (CPI)

A formal implementation of this methodology is a process

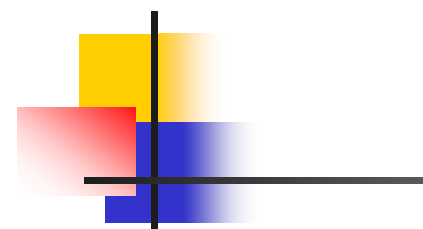


Table 2-2: Type of Plans

Plan	Purpose	Scope	Plan Relationship
Business Continuity Plan (BCP)	Provides procedures for sustaining mission/business operations from	Addresses mission/business processes at a lower or	Mission/business process focused plan that may be
Continuity of Operations (COOP) Plan	Proguic org; alte day dire		
Crisis Communications Plan	Pro diss exte me; stat rum		
Critical Infrastructure Protection (CIP) Plan	Pro pro nati con the Pro		
Cyber Incident Response Plan	Pro miti cyb wor		
Disaster Recovery Plan (DRP)	Pro relo systems operations to an alternate location.		
Information System Contingency Plan (ISCP)	Provides procedures and capabilities for recovering an information system.	Addresses single information system recovery at the current or, if appropriate alternate location.	Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP.
Occupant Emergency Plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat.	Focuses on personnel and property particular to the specific facility; not mission/business process or information system-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

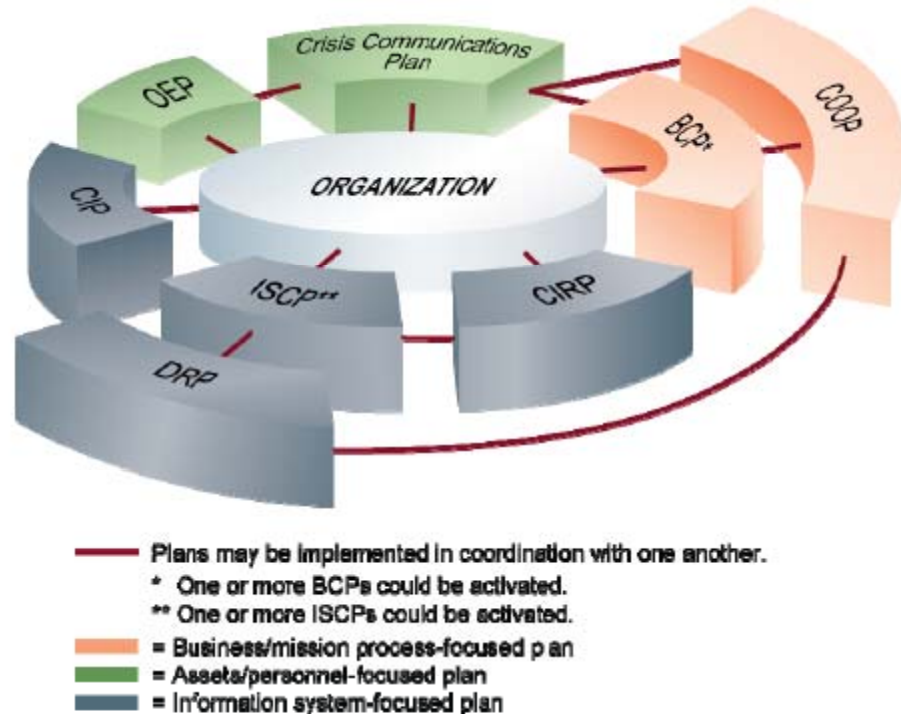


Figure 2-1: Contingency-Related Plan Relationships

NIST SP 800-34 CP

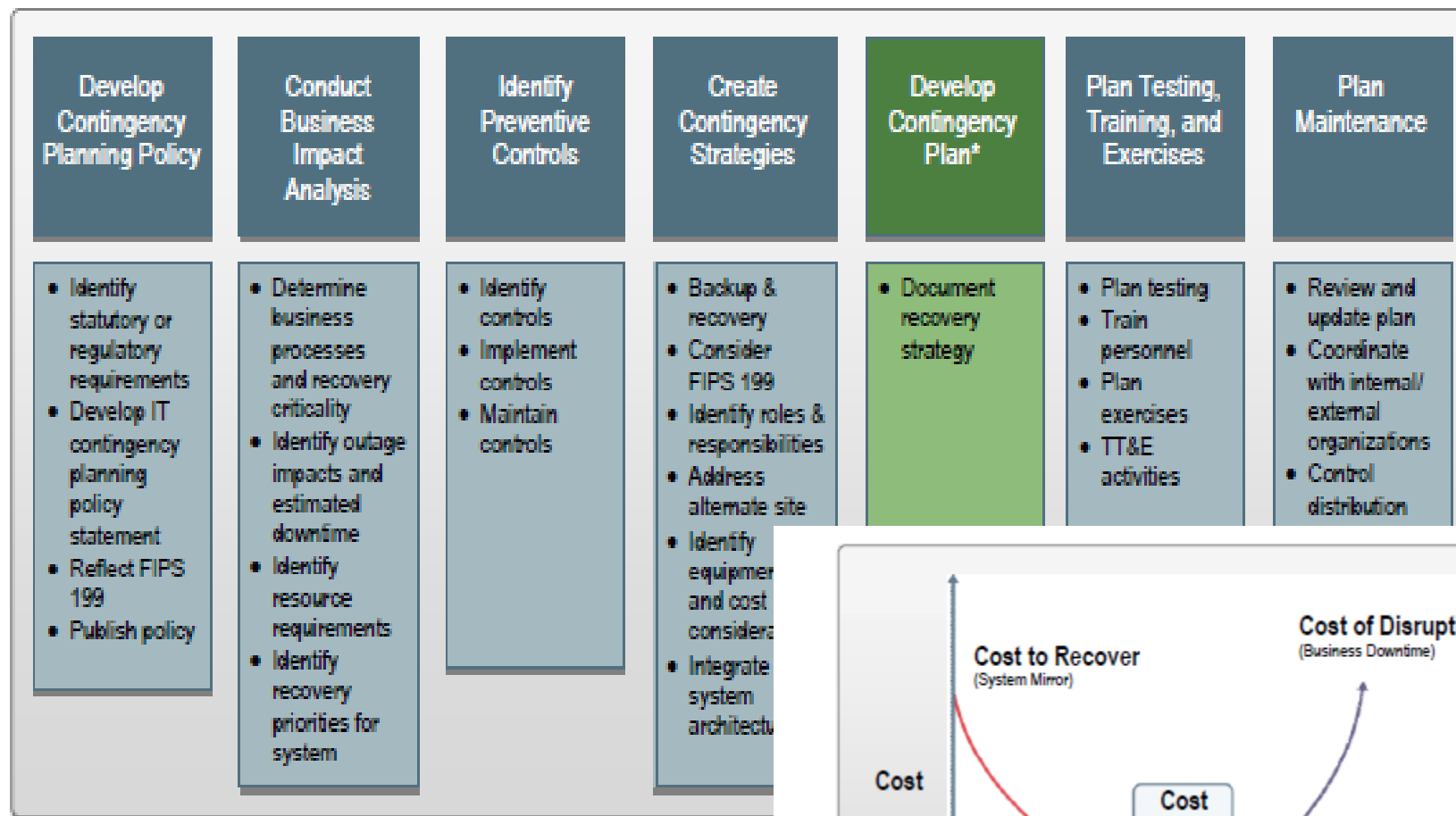
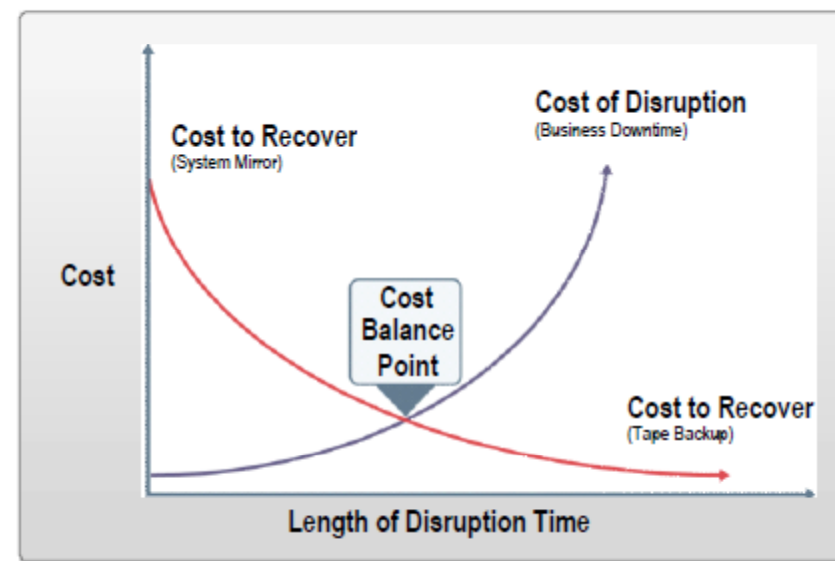


Figure 3-1: Contingency Planning Process



NIST SP 800-34 CP

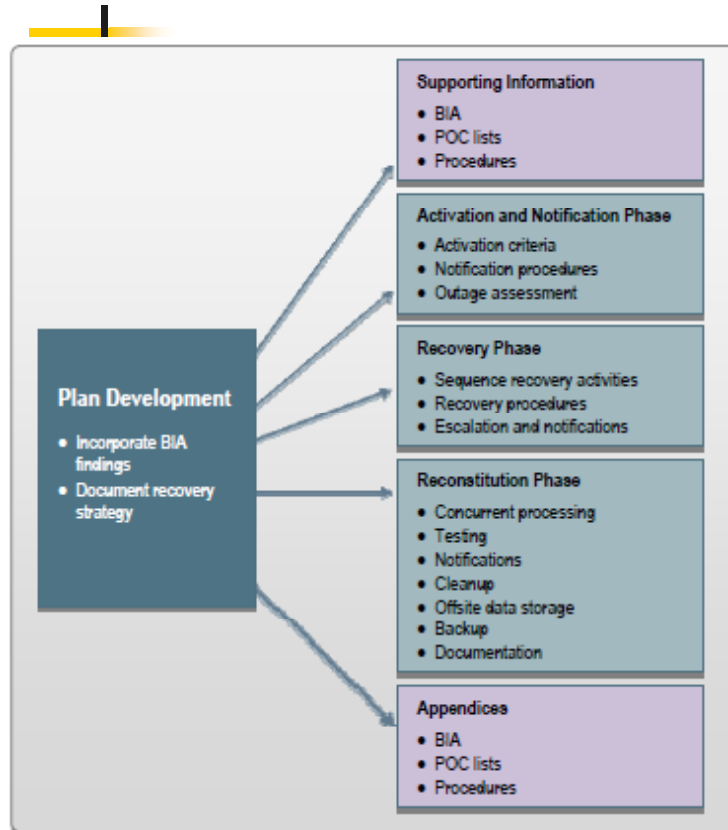


Figure 4-1: Contingency Plan Structure

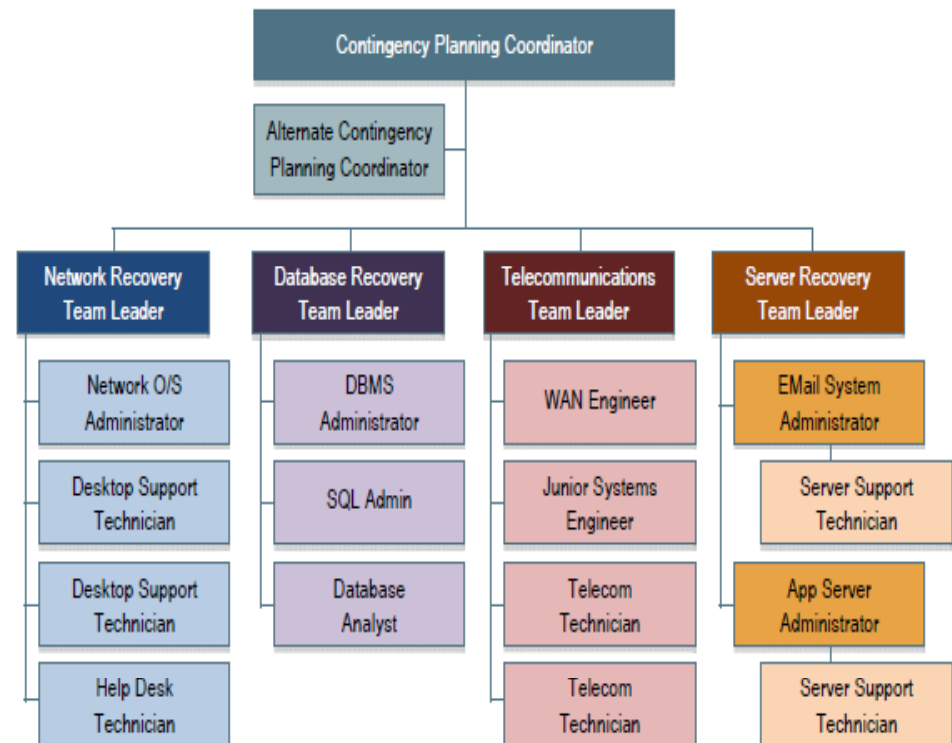
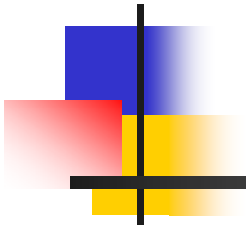


Figure 4-2: Sample Call Tree

Read Sample Information Security Contingency Plan



Information Security Policy



Introduction

- Information security policy:
 - What it is
 - How to write it
 - How to implement it
 - How to maintain it
- Policy
 - Essential foundation of effective information security program

Why Policy?

- A quality information system
 - begins and ends with policy
 - least expensive means to implement
- Some basic rules must be followed
 - Never conflict with law
 - Stand up in court
 - Properly supported and administered
- Some Guidelines
 - It should contribute to the success of the organization
 - Management must ensure the adequate sharing of responsibility for proper use of information systems
 - Involve end users of information systems

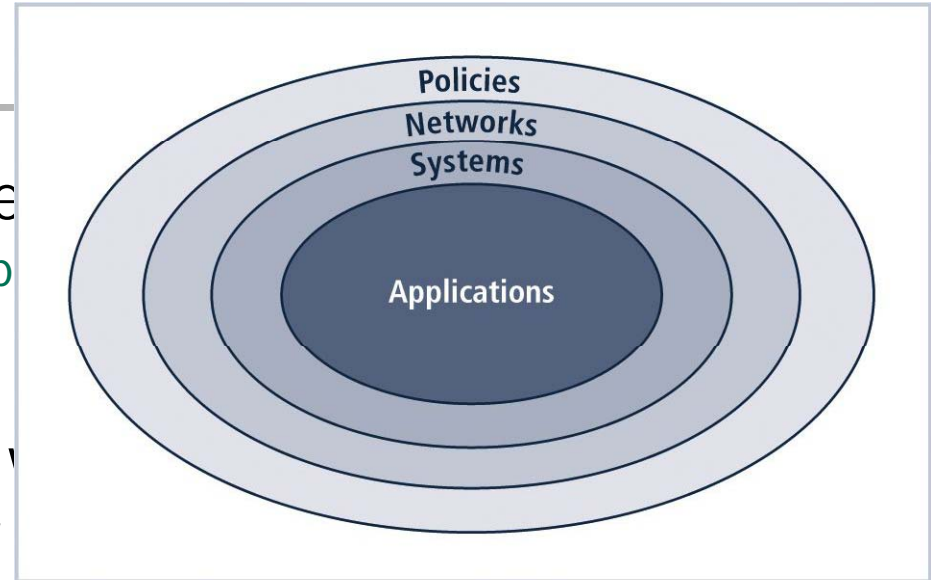


FIGURE 4-1 The Bull's-Eye Model

Policies, Standards, & Practices

Policy: A set of rules that dictates acceptable and unacceptable behavior

Standards: more detailed statement of what must be done to comply with policy

Practices, procedures and guidelines: explain how employees will comply with policy

- Policies must be:
 - Properly disseminated
 - Read
 - Understood
 - Agreed-to
 - constantly updated

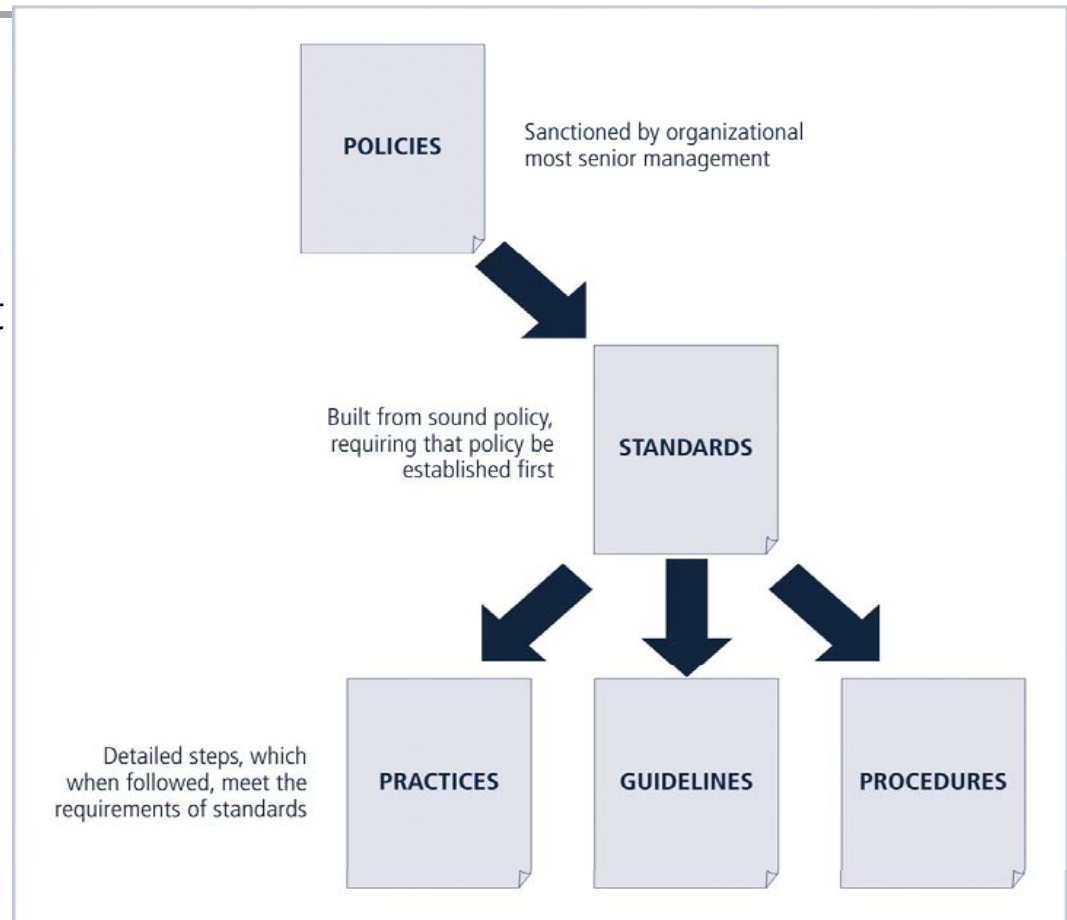


FIGURE 4-2 Policies, Standards, and Practices



Policy, Standards, and Practices (Continued)

- Define three types of information security policy (NIST 800-14):
 - Enterprise information security program policy
 - Issue-specific information security policies
 - Systems-specific information security policies



Enterprise Information Security Policy (EISP)

- Sets strategic direction, scope, and tone for organization's security efforts
 - Executive-level document; 2-10 pages
 - CISO in consultation with CIO
- Assigns responsibilities for various areas of information security, including
 - Maintenance of information security policies
 - Practices and responsibilities of end users
- EISP guides
 - The development, implementation, and management requirements of information security program



EISP Elements

- EISP documents **should** provide :
 - An overview of corporate philosophy on security
 - Information about information security organization and information security roles
 - Responsibilities for security shared by all members of the organization
 - Responsibilities for security unique to each role within the organization



Components of the EISP

- Statement of Purpose:
 - What the policy is for
- Information Technology Security Elements:
 - Defines information security / clarify philosophies
- Need for Information Technology Security:
 - justifies importance of information security in the organization
- Information Security Responsibilities and Roles:
 - Defines organizational structure
- References Information Technology standards and guidelines



Example EISP

- Protection Of Information:
 - Information must be protected in a manner commensurate with its sensitivity, value, and criticality
- Use Of Information:
 - Company X information must be used only for business purposes expressly authorized by management
- Information Handling, Access, And Usage:
 - Information is a vital asset and all accesses to, uses of, and processing of Company X information must be consistent with policies and standards



Example EISP – CCW (Continued)

- Data And Program Damage Disclaimers:
 - Company X disclaims any responsibility for loss or damage to data or software that results from its efforts to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems
- Legal Conflicts
- Exceptions To Policies
- Policy Non-Enforcement
- Violation Of Law
- Revocation Of Access Privileges
- Industry-Specific Information Security Standards
- Use Of Information Security Policies And Procedures
- Security Controls Enforceability



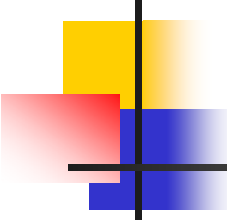
Issue-Specific Security Policy (ISSP)

- Every organization's ISSP has three characteristics:
 - Addresses specific technology-based systems
 - Requires frequent updates
 - Contains an issue statement on the organization's position on an issue
- ISSP topics could include:
 - E-mail use,
 - Internet and World Wide Web use,
 - Specific minimum configurations of computers to defend against worms and viruses,
 - Prohibitions against hacking or testing organization security controls,
 - ..



Typical ISSP Components

- Statement of Purpose
 - Scope and Applicability
 - Definition of Technology Addressed
 - Responsibilities
- Authorized Access and Usage of Equipment
 - User Access
 - Fair and Responsible Use
 - Protection of Privacy
- Prohibited Usage of Equipment
 - Disruptive Use or Misuse
 - Criminal Use
 - Offensive or Harassing Materials
 - Copyrighted, Licensed or other Intellectual Property
 - Other Restrictions



Components of the ISSP (Continued)

- Systems Management
 - Management of Stored Materials
 - Employer Monitoring
 - Virus Protection
 - Physical Security
 - Encryption
- Violations of Policy
 - Procedures for Reporting Violations
 - Penalties for Violations
- Policy Review and Modification
 - Scheduled Review of Policy and Procedures for Modification
- Limitations of Liability
 - Statements of Liability or Disclaimers



Implementing ISSP

- Common approaches include creating:
 - a number of independent ISSP documents
 - a single comprehensive ISSP document
 - A modular ISSP document that unifies policy creation and administration
 - Recommended approach
 - It provides a balance between issue orientation and policy management

TABLE 4-4 ISSP Approaches

Approach	Advantages	Disadvantages
Individual Policy	Clear assignment to a responsible department Written by those with superior subject matter expertise for technology-specific systems	Typically yields a scattershot result that fails to cover all of the necessary issues Can suffer from poor policy dissemination, enforcement, and review
Comprehensive Policy	Well controlled by centrally managed procedures assuring complete topic coverage Often provides better formal procedures than when policies are individually formulated Usually identifies processes for dissemination, enforcement, and review	May over-generalize the issues and skip over vulnerabilities May be written by those with less complete subject matter expertise
Modular Policy	Often considered an optimal balance between the individual ISSP and the comprehensive ISSP approaches Well controlled by centrally managed procedures, assuring complete topic coverage Clear assignment to a responsible department Written by those with superior subject matter expertise for technology-specific systems	May be more expensive than other alternatives Implementation can be difficult to manage



Systems-Specific Policy (SysSP)

- Systems-Specific Policies (SysSPs)
 - May not look like other types of policy
- They may often be created to function as
 - standards or procedures to be used when configuring or maintaining systems
- SysSPs can be separated into:
 - Management guidance
 - Technical specifications
 - Maybe combined in a single policy document



Systems-Specific Policy (SysSP)

- Management Guidance SysSPs

- Created by management
 - guides the implementation and configuration of technology
- Applies to any technology that affects the confidentiality, integrity or availability of information
- Informs technologists of management intent

- Technical Specifications SysSPs

- System administrators' directions on implementing managerial policy
- Each type of equipment has its own type of policies
- Two general methods of implementing such technical controls:
 - Access control lists
 - Configuration rules

Combined Document

- Often combine these two in one
 - Practical but can be confusing
 - Care should be taken



Access Control Lists

- Include user access lists, matrices, and capability tables that govern rights and privileges
- Can control access to file storage systems, object brokers or other network communications devices
- ACLs enable administrations to restrict access according to user, computer, time, duration, etc.
- Capability Table:
 - similar method that specifies which subjects and objects users or groups can access
- Specifications are frequently complex matrices, rather than simple lists or tables



Configuration Rules

- Configuration rules
 - specific configuration codes entered into security systems to guide execution of system when information passes through it
- Rule-based policies
 - more specific to system operation than ACLs and may or may not deal with users directly
- Many security systems require
 - specific configuration scripts telling systems what actions to perform on each set of information processed



Guidelines for Policy Development

- View PD as a two-part project
 1. Design and develop policy (or redesign and rewrite outdated policy)
 2. Establish management processes to perpetuate policy within organization



The Policy Project

- Policy (re)development projects should be
 - well planned,
 - properly funded, and
 - aggressively managed to ensure completion on time and within budget
- Policy development project can be guided by the SecSDLC process
 - Investigation
 - Analysis
 - Design
 - Implementation
 - Maintenance



Investigation Phase

- The policy development team should:
 - Obtain support from senior management (CIO)
 - Clearly articulate goals of policy project
 - Gain participation of correct individuals affected by recommended policies
 - Be composed from Legal, Human Resources and end-users
 - Assign project **champion** with sufficient stature and prestige
 - Acquire a capable project manager
 - Develop detailed outline of and sound estimates for the cost and scheduling of the project



Analysis Phase

- Analysis phase should include the following activities:
 - New or recent risk assessment or IT audit
 - document the current information security needs of the organization
 - Key reference materials—including any existing policies



Design Phase

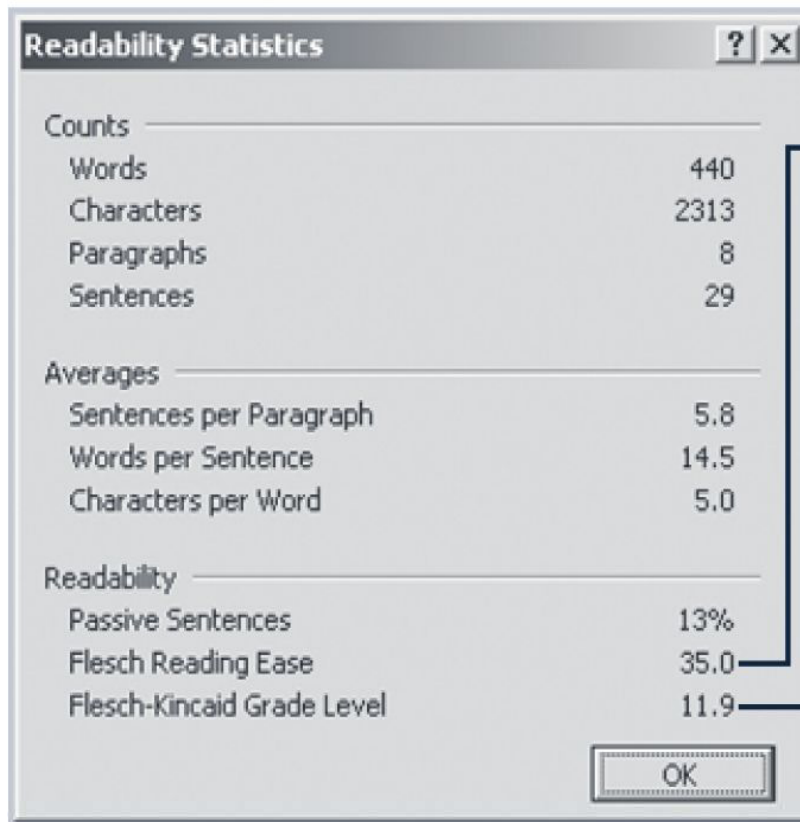
- Design phase should include:
 - How policies will be distributed
 - How verification of distribution will be accomplished
 - Specifications for any automated tools
 - Revisions to feasibility analysis reports based on improved costs and benefits as design is clarified



Implementation Phase

- Implementation Phase:
 - Writing the policies
- Make certain policies are enforceable as written
- Policy distribution is not always as straightforward
- Effective policy
 - Is written at a reasonable reading level
 - Readability statistics
 - Attempts to minimize technical jargon and management terminology

Readability Statistics Example



The Flesch Reading Ease scale evaluates the writing on a scale of 1 to 100. The higher the score, the easier it is to understand the writing.

This score is too complex for most policies, but appropriate for a college text. For most corporate documents, a score of 60 to 70 is preferred.

The Flesch-Kincaid Grade Level score evaluates writing on a U.S. grade-school level.

While an eleventh to twelfth grade level may be appropriate for this book, it is too high for an organization's policy.

For most corporate documents, a score of 7.0 to 8.0 is preferred.

FIGURE 4-9 Readability Statistics for Policy

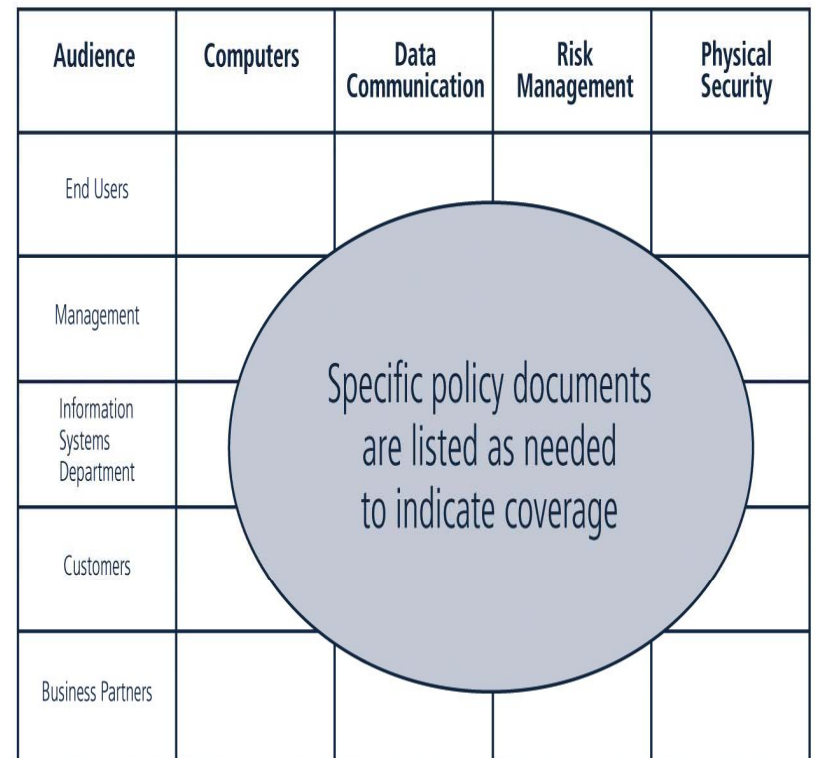


Maintenance Phase

- Maintain and modify policy as needed
 - to ensure that it remains effective as a tool to meet changing threats
- Policy should have a built-in mechanism
 - To support users to report problems with the policy, preferably anonymously
- Periodic review should be built in to the process

The Information Security Policy Made Easy Approach (ISPME)

- Gathering Key Reference Materials
- Defining A Framework For Policies
- Preparing A Coverage Matrix
- Making Critical Systems Design Decisions
- Structuring Review, Approval, And Enforcement Processes



Audience	Computers	Data Communication	Risk Management	Physical Security
End Users				
Management				
Information Systems Department				
Customers				
Business Partners				

FIGURE 4-11 A Sample Coverage Matrix



ISPME Checklist

- Perform risk assessment or information technology audit to determine your organization's unique information security needs
- Clarify what “policy” means within your organization so that you are not preparing a “standard,” “procedure,” or some other related material
- Ensure that roles and responsibilities related to information security are clarified, including responsibility for issuing and maintaining policies
- Convince management that it is advisable to have documented information security policies
 - And so on ..
- (Refer to the huge checklist!!)



ISPME Next Steps

- Post Policies To Intranet Or Equivalent
- Develop A Self-Assessment Questionnaire
- Develop Revised user ID Issuance Form
- Develop Agreement To Comply With Information Security Policies Form
- Develop Tests To Determine If Workers Understand Policies
- Assign Information Security Coordinators
- Train Information Security Coordinators



ISPME Next Steps (Continued)

- Prepare And Deliver A Basic Information Security Training Course
- Develop Application Specific Information Security Policies
- Develop A Conceptual Hierarchy Of Information Security Requirements
- Assign Information Ownership And Custodianship
- Establish An Information Security Management Committee
- Develop An Information Security Architecture Document



SP 800-18: Guide for Developing Security Plans

- NIST Special Publication 800-18 offers another approach to policy management
- Policies:
 - Documents that constantly change/grow
 - Must be properly disseminated (distributed, read, understood and agreed to) and managed



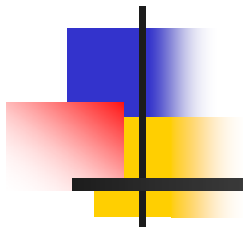
SP 800-18: Guide for Developing Security Plans (Continued)

- Good management practices for policy development and maintenance make for a more resilient organization
- In order to remain current and viable, policies must have:
 - Individual responsible for reviews
 - Schedule of reviews
 - Method for making recommendations for reviews
 - Indication of policy and revision date



Summary

- It is important to emphasize the preventative nature of policy
- Policies exist first, and foremost,
 - to inform employees of what is and is not acceptable behavior in the organization
- Policy seeks to improve
 - employee productivity, and prevent potentially embarrassing situations



Developing the Security Program



Introduction

- Security programs
 - describe the entire set of personnel, plans, policies, and initiatives related to information security
- Information security program
 - describe the structure and organization of the effort that contains risks to the information assets of organization



Organizing for Security

- Some variables that determine how to structure an information security program are:
 - Organizational culture
 - Size
 - Security personnel budget
 - Security capital budget



Security in Large Organizations

- InfoSec departments in large organizations
 - tend to form and re-form internal groups to meet long-term challenges
 - Functions are likely to be split into groups
- InfoSec departments in small organizations
 - typically create fewer groups, perhaps only having one general group of specialists



Large Organizations

With 1,000 to 10,000 computers

- At this size,
 - approach to security is often matured,
 - Integration of planning and policy into organization's culture
- Unfortunately, large organization does not always put
 - large amounts of resources into security considering vast numbers of computers and users
 - Tend to spend proportionally less on security



Very Large Organizations

More than 10,000 Computers

- Security budgets often grow faster than IT budgets
- Even with large budgets, average amount spent on security per user is still smaller than any other type of organization

Where small orgs spend more than \$5,000 per user on security, very large organizations spend about 1/18th of that, roughly \$300 per user

- Does a better job in the policy and resource mgmt areas, although only 1/3 of organizations handled incidents according to an IR plan

TABLE 5-1 Functions Needed to Implement the Information Security Program

Function	Description	Comments
Risk Assessment	Evaluates risk present in IT initiatives and/or systems	Identifies the sources of risk and may offer advice on controls that can reduce risk
Risk Management	Implements or oversees use of controls to reduce risk	Often paired with risk assessment
Systems Testing	Evaluates patches used to close software vulnerabilities and acceptance testing of new systems to assure compliance with policy and effectiveness	Usually part of the incident response and/or risk management functions
Policy	Maintains and promotes information security policy across the organization	Must be coordinated with organization-wide policy processes
Legal Assessment	Maintains awareness of planned and actual laws and their impact, and coordinates with outside legal counsel and law enforcement agencies	Almost always external to the information security and IT departments
Incident Response	Handles the initial response to potential incidents, manages escalation of actual incidents, and coordinates the earliest responses to incidents and disasters	Often cross-functional and drawn from multiple departments; should include middle management to manage escalation processes
Planning	Researches, creates, maintains, and promotes information security plans; often takes a project management approach to planning as contrasted with strategic planning for the whole organization	Must coordinate with organization-wide policy processes
Measurement	Uses existing control systems (and perhaps specialized data collection systems) to measure all aspects of the information security environment	Management relies on timely and accurate statistics to make informed decisions

TABLE 5-1 Functions Needed to Implement the Information Security Program (continued)

Function	Description	Comments
Compliance	Verifies that system and network administrators repair identified vulnerabilities promptly and correctly	Poses problems for good customer service because it is difficult to be customer-focused and to enforce compliance at the same time
Centralized Authentication	Manages the granting and revocation of network and system credentials for all members of the organization	Often delegated to the help desk or staffed in conjunction and co-located with the help desk function
Systems Security Administration	Administers the configuration of computer systems, which are often organized into groups by the operating system they run	Many organizations may have originally assigned all security functions to these groups outside of the information security function; this can be a source of conflict when organizations update their information security program
Training	Trains general staff in information security topics, IT staff in specialized technical controls, and internal information security staff in specialized areas of information security, including both technical and managerial topics	Some or all of this function may be carried out in conjunction with the corporate training department
Network Security Administration	Administers configuration of computer networks, often organized into groups by logical network area (i.e., WAN, LAN, DMZ) or geographic location	Many organizations may have originally assigned some security functions to these groups outside of the information security function, which may require close coordination or reassignment
Vulnerability Assessment	Locates exposure within information assets so these vulnerabilities can be repaired before weaknesses are exploited	Sometimes called the penetration testing team or the ethical hacking unit; often outsourced to consultant "tiger teams"

Suggested Functions Needed to Implement InfoSec Program



Security in Large Organizations

- Recommended approach: separate into 4 areas:
 - Functions performed by **non-technology business** units outside of IT
 - Legal; Training
 - Functions performed by **IT groups outside of information security** area of management control
 - Network/systems security administrator
 - Centralized authentication
 - Functions performed **within information security department** as **customer service**
 - Risk assessment; systems testing; incident response; planning; measurement; vulnerability assessment
 - Functions performed **within the information security department** as **compliance enforcement obligation**
 - Policy; compliance; risk management



Responsibilities in Large Organizations

- CISO's responsibility - see that
 - information security functions are adequately performed somewhere within the organization
- Deployment of full-time security personnel depends on a number of factors,
 - sensitivity of information to be protected,
 - industry regulations and
 - general profitability

Typical Information Security Staffing in a Large Organization

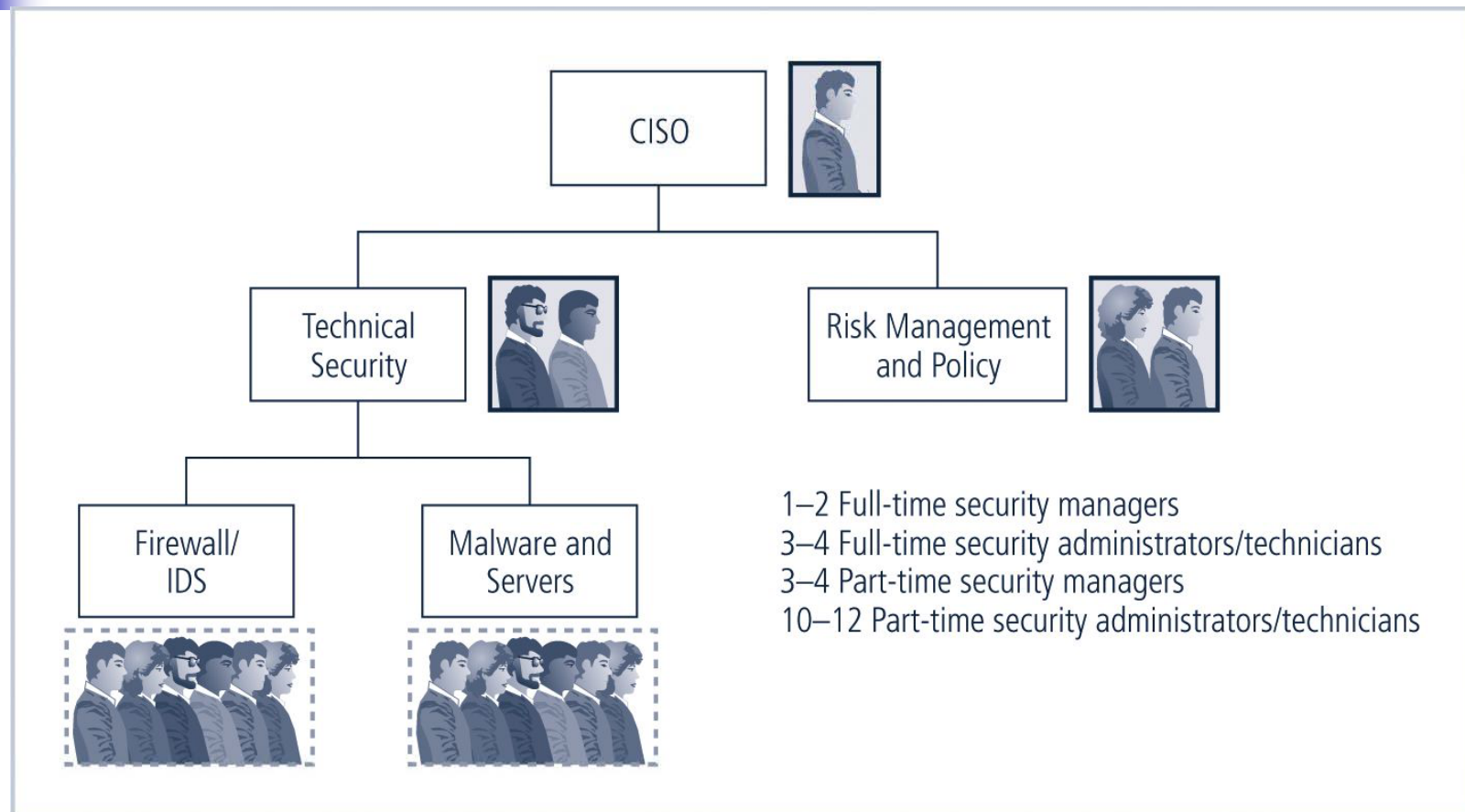


FIGURE 5-1 Information Security Staffing in a Large Organization

Typical InfoSec Staffing in a Very Large Organization

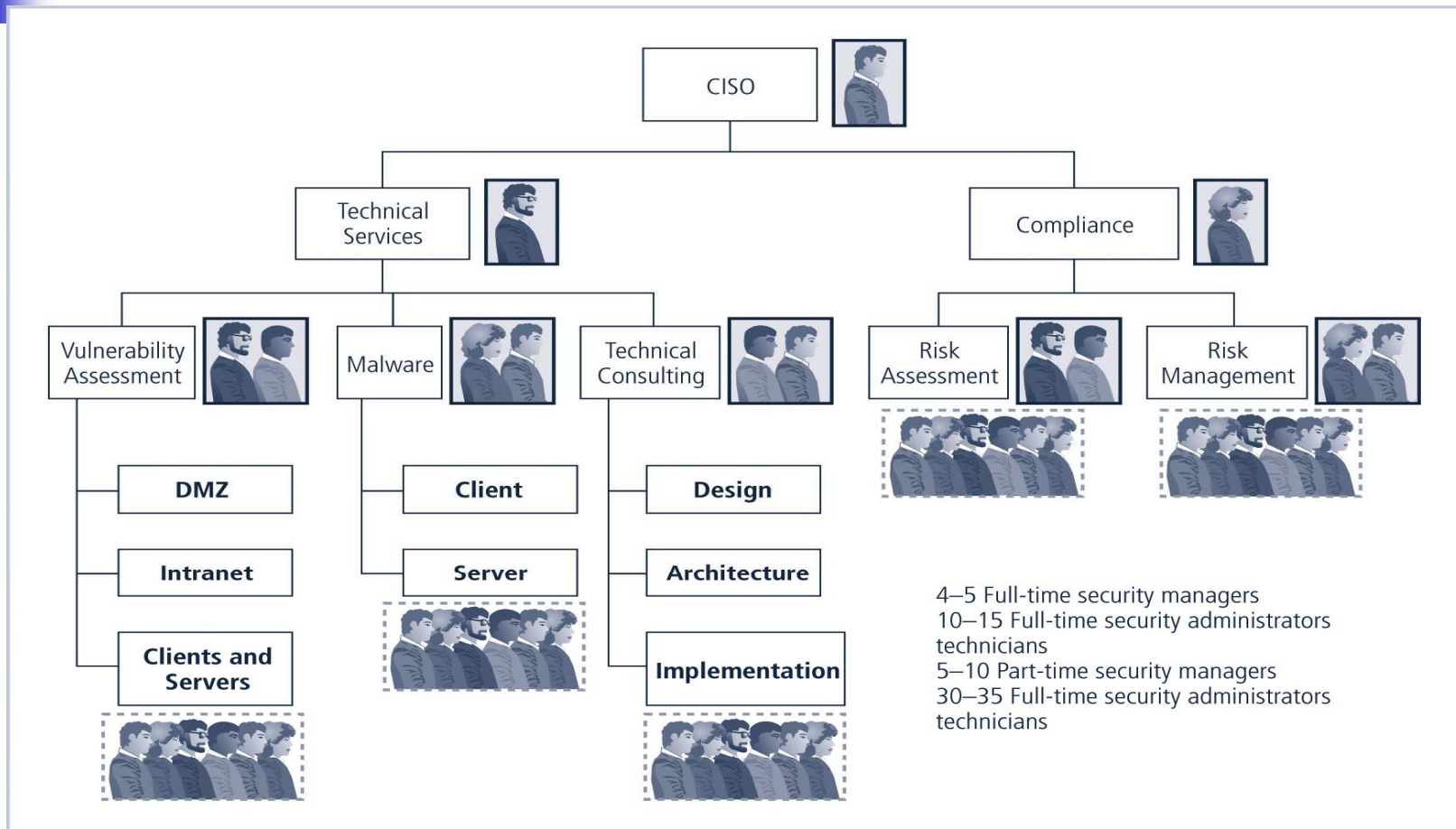


FIGURE 5-2 Information Security Staffing in a Very Large Organization



Security in Medium-Sized Organizations (100-1,000 PCs)

- Have smaller total budget
- May have same sized security staff as small org, but larger need
- Typically relies on help from IT staff for plans and practices
- May be large enough
 - to implement multi-tiered approach to security
 - with fewer dedicated groups and more functions assigned to each group
- Medium-sized organizations tend to ignore some security functions.

Typical InfoSec Staffing in a Medium Organization

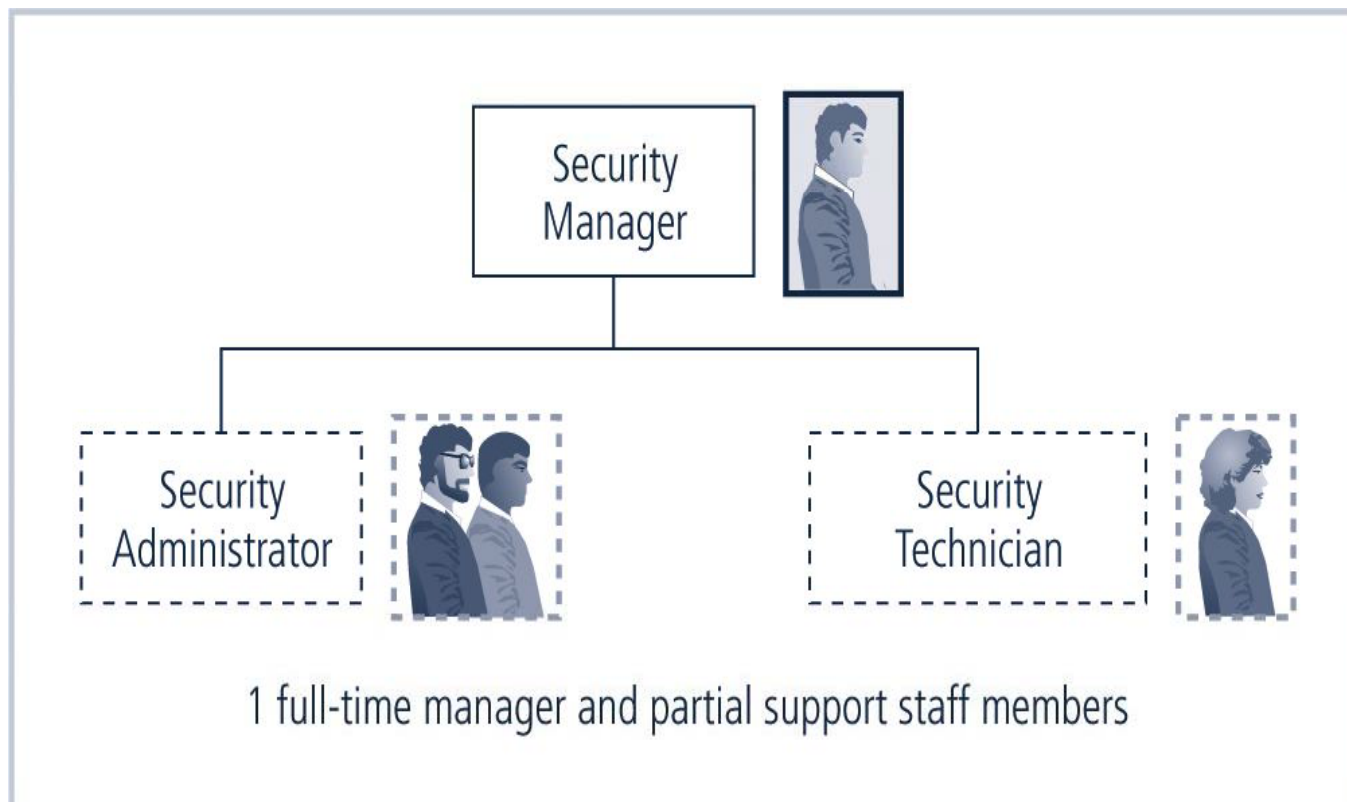


FIGURE 5-3 Information Security Staffing in a Medium-Sized Organization

Security in Small Organizations

10-100 Computers

- Have simple, centralized IT organizational model
- Spend disproportionately more on security
- Information security in small org is often responsibility of a **single security administrator**
- Such organizations frequently have little in the way of formal policy, planning, or security measures
 - Commonly outsource their Web presence or electronic commerce operations
 - Security training and awareness is commonly conducted on a 1-on-1 basis
 - Policies are often issue-specific
 - Formal planning is often part of IT planning
- Threats from insiders are less likely in such an environment

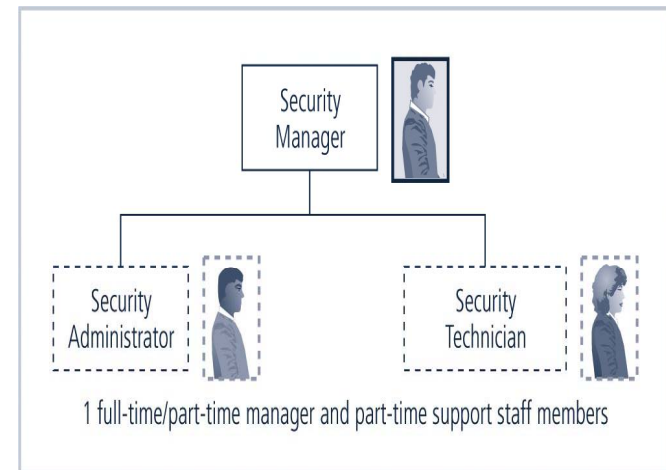


FIGURE 5-4 Information Security Staffing in a Smaller Organization



Placing Information Security Within An Organization

- In large organizations,
 - InfoSec is often located within IT department,
 - headed by CISO who reports directly to top computing executive, or CIO
- By its very nature, an InfoSec program is **sometimes at odds** with the goals and objectives of the IT department as a whole



Placing Information Security Within An Organization (Continued)

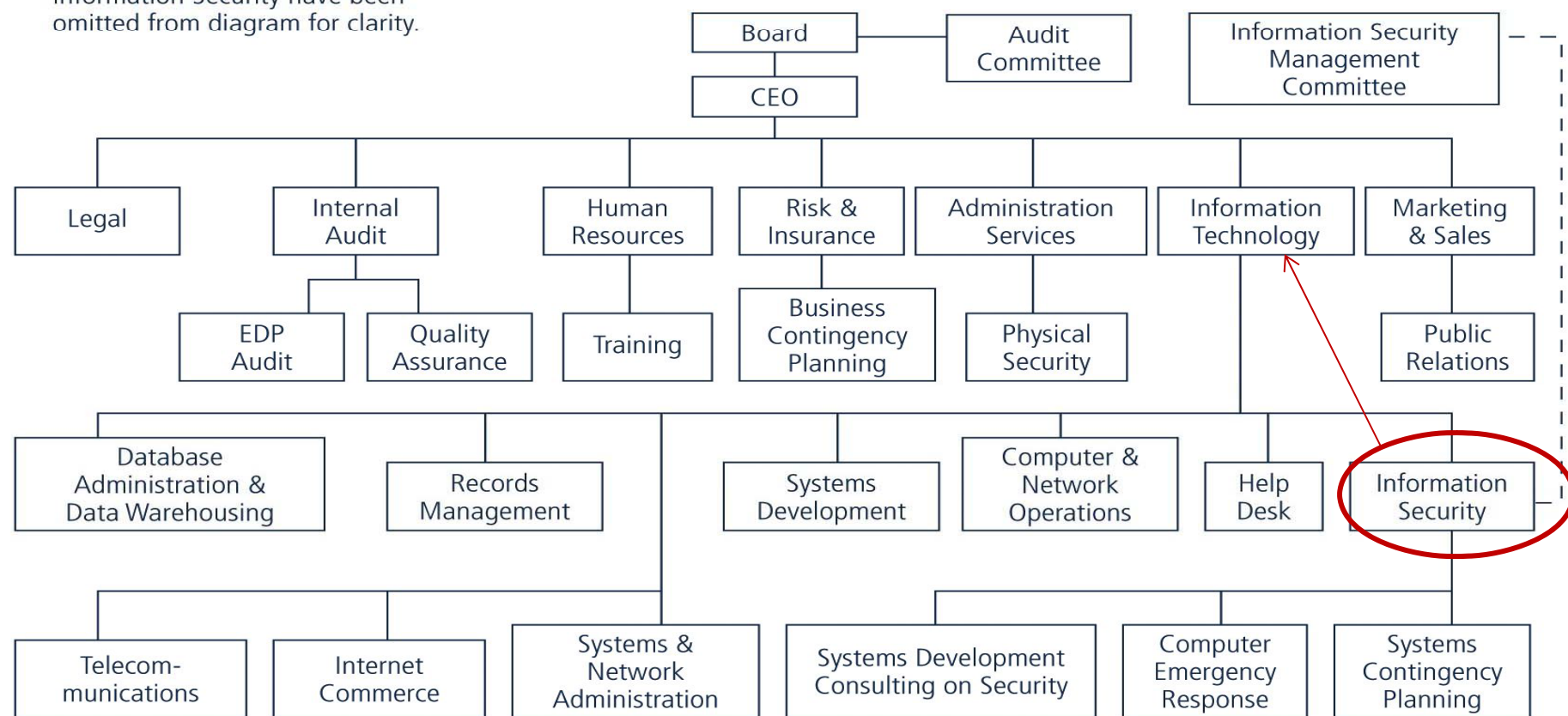
- Possible conflicts between CIO/CISO goals
 - Current movement to separate information security from IT division
- The challenge is
 - to design a reporting structure for the InfoSec program that balances the needs of each of the communities of interest

IT Department

Departments not related to Information Security have been omitted from diagram for clarity.

Maybe some Col between IT and IS

Over 50% use this

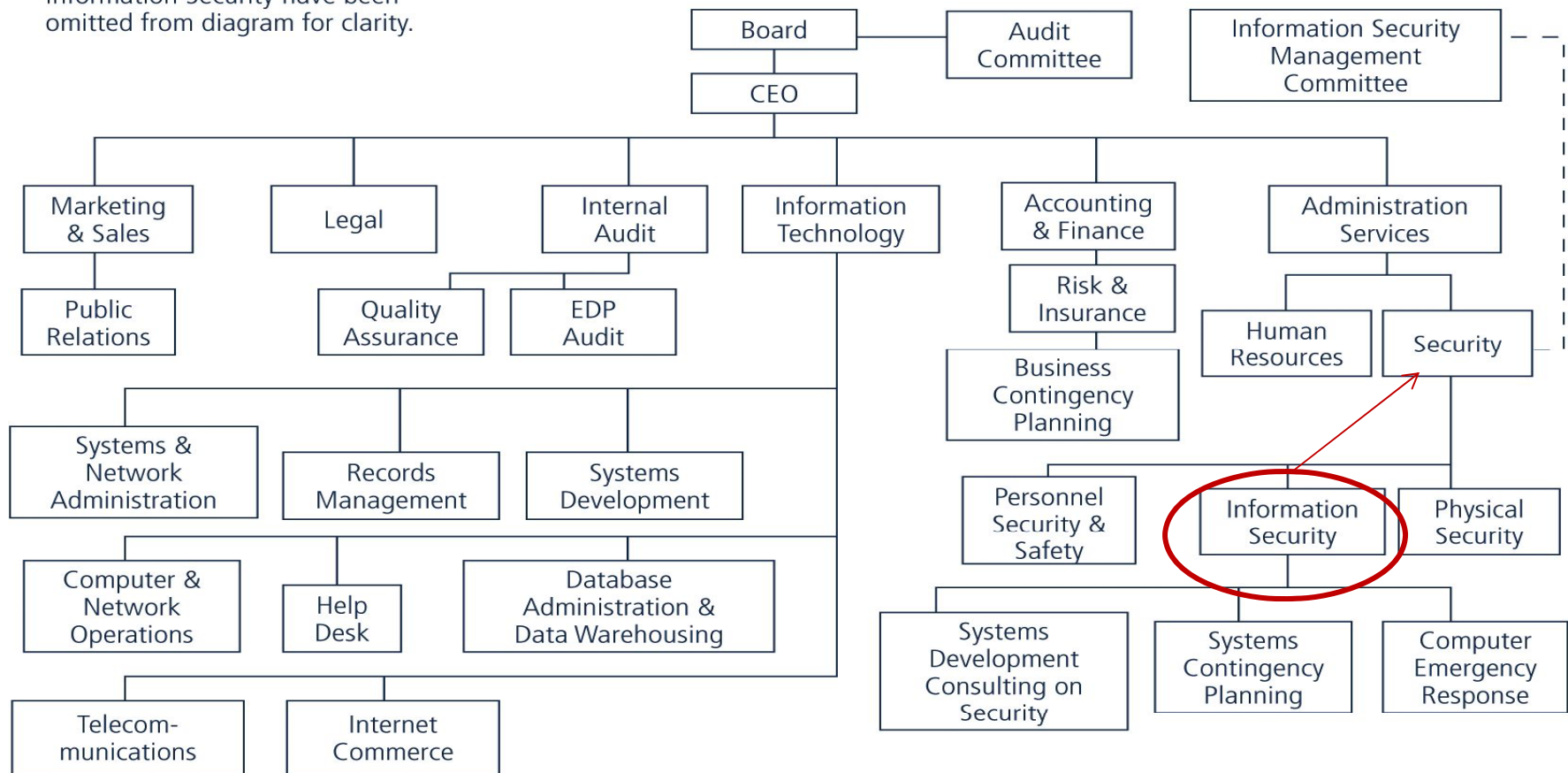


From *Information Security Roles and Responsibilities Made Easy*, used with permission.

FIGURE 5-5 Wood's Option 1: Information Security Reports to Information Technology Department

Broadly Defined Security Department

Departments not related to Information Security have been omitted from diagram for clarity.

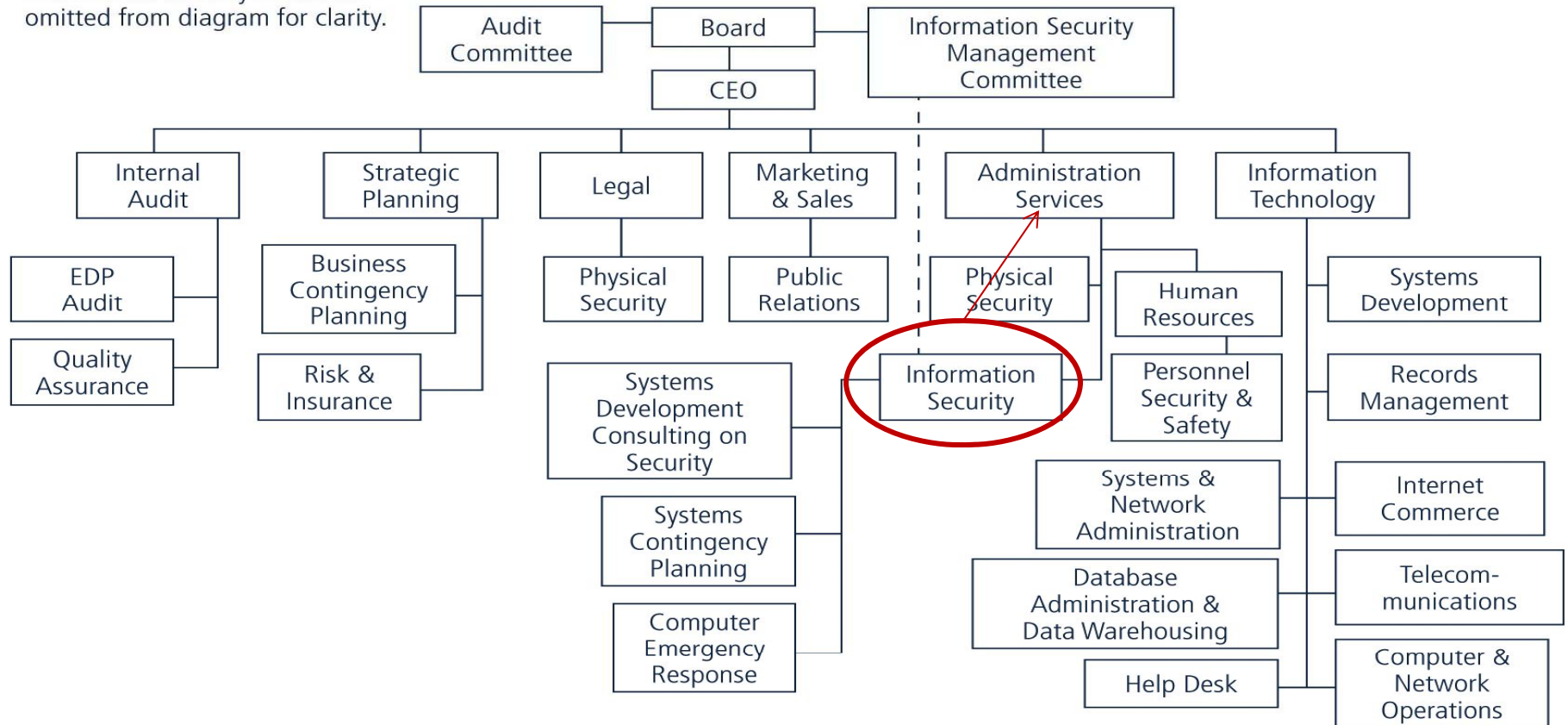


From *Information Security Roles and Responsibilities Made Easy*, used with permission.

FIGURE 5-6 Wood's Option 2: Information Security Reports to Broadly Defined Security Department

Administrative Services Department

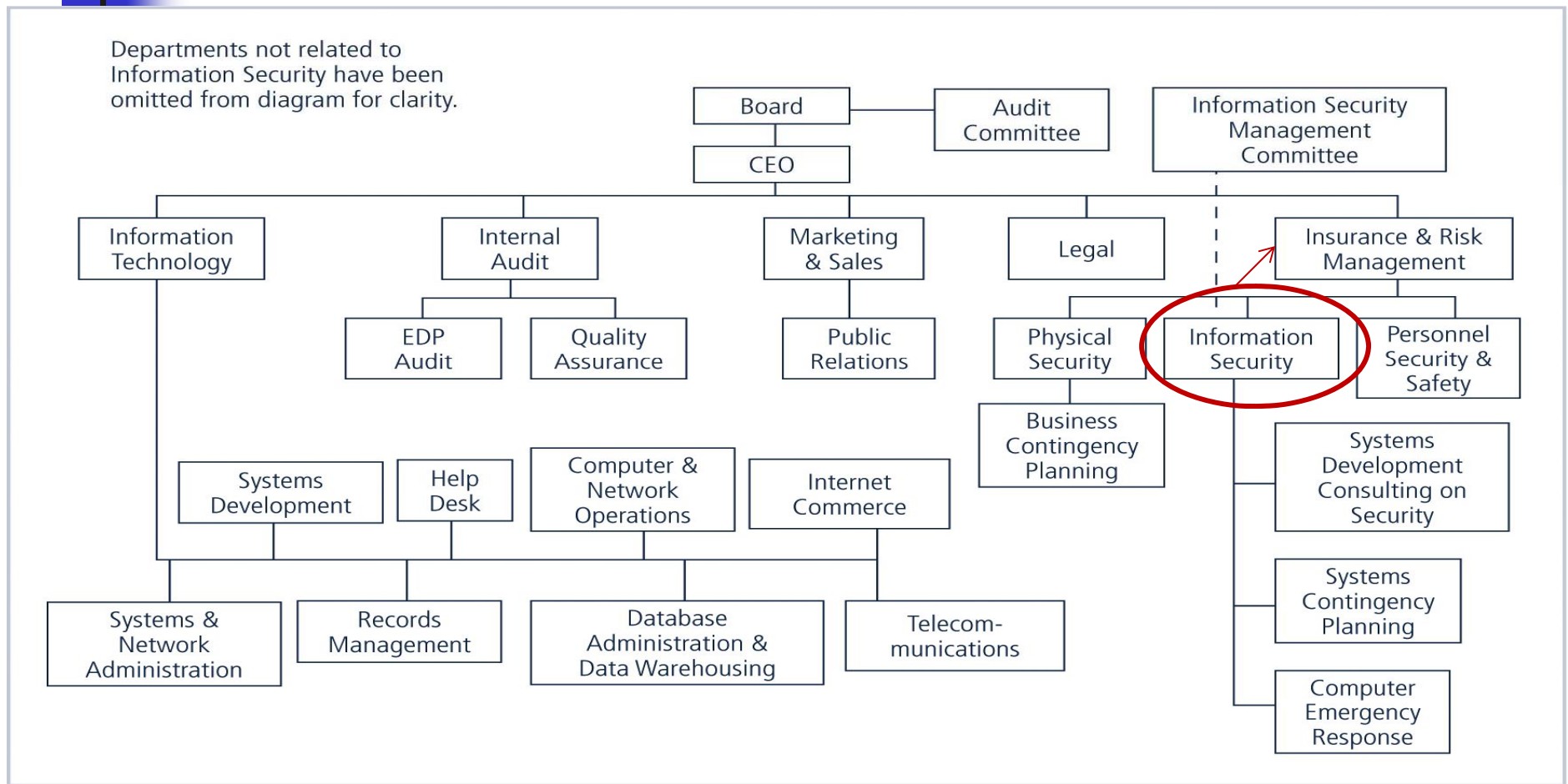
Departments not related to Information Security have been omitted from diagram for clarity.



From *Information Security Roles and Responsibilities Made Easy*, used with permission.

FIGURE 5-7 Wood's Option 3: Information Security Reports to Administrative Services Department

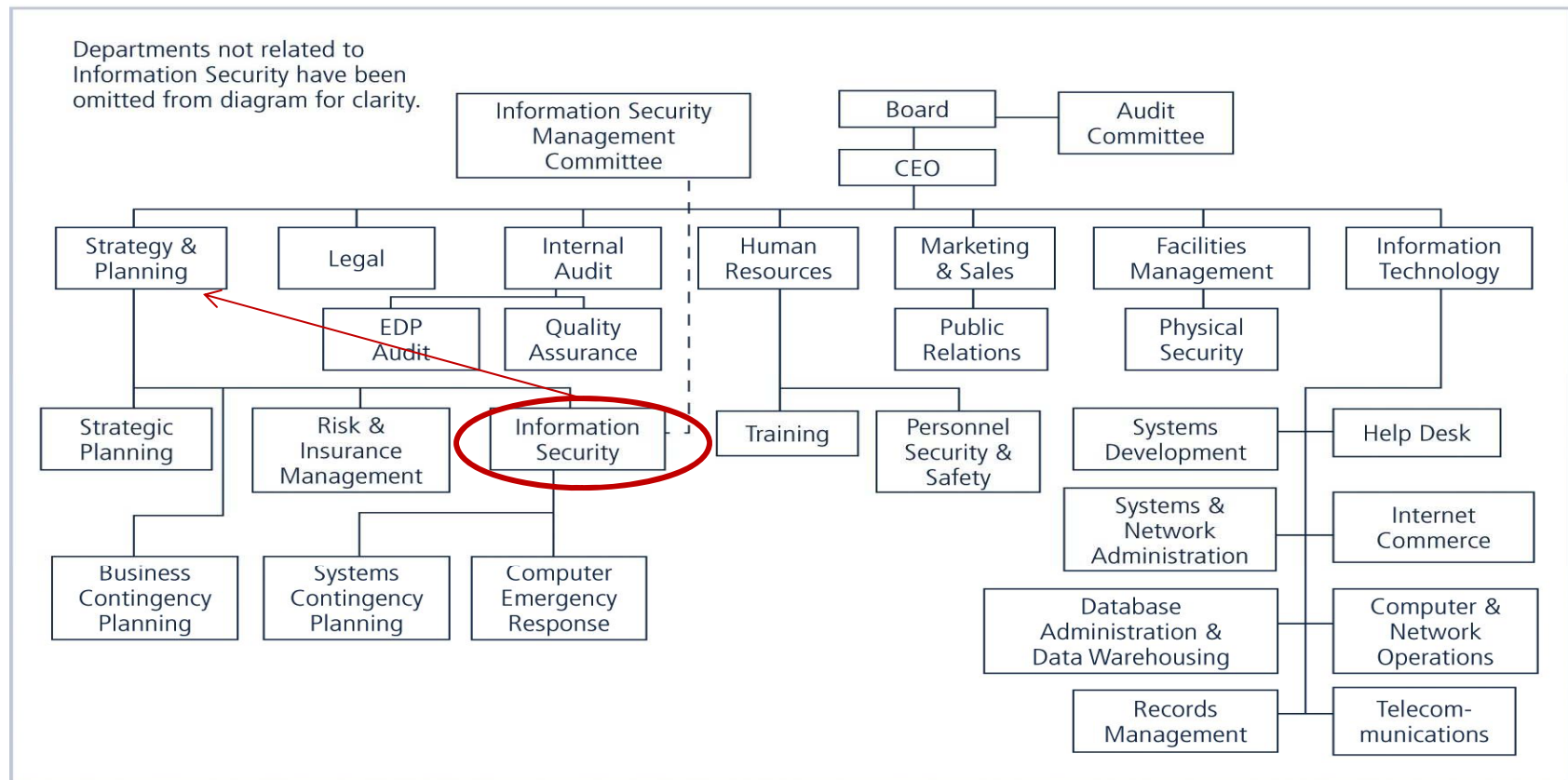
Insurance & Risk Mgmt Department



From *Information Security Roles and Responsibilities Made Easy*, used with permission.

FIGURE 5-8 Wood's Option 4: Information Security Reports to Insurance and Risk Management Department

Strategy & Planning Department

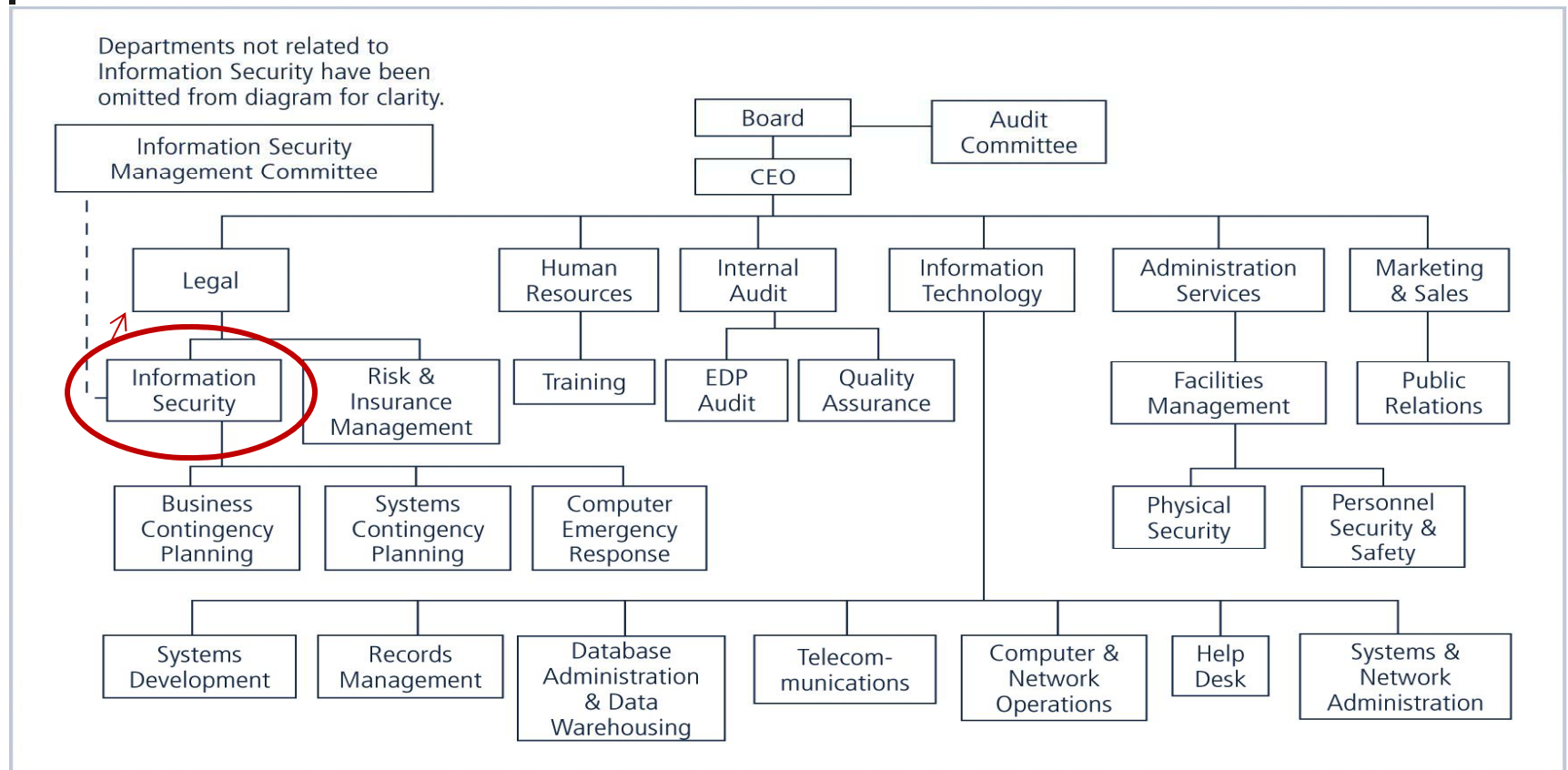


From *Information Security Roles and Responsibilities Made Easy*, used with permission.

FIGURE 5-9 Wood's Option 5: Information Security Reports to Strategy and Planning Department

From *Information Security Roles and Responsibilities Made Easy*

Legal Department



From *Information Security Roles and Responsibilities Made Easy*, used with permission.

FIGURE 5-10 Wood's Option 6: Information Security Reports to Legal Department

From *Information Security Roles and Responsibilities Made Easy*, used with permission.



Other Options

- Option 7: Internal Audit
- Option 8: Help Desk
- Option 9: Accounting and Finance Through IT
- Option 10: Human Resources
- Option 11: Facilities Management
- Option 12: Operations



Components of the Security Program

- Determining what level the information security program operates on depends on the organization's strategic plan
 - In particular, on the plan's vision and mission statements
- The CIO and CISO should use these two documents to formulate the mission statement for the information security program
 - NIST SP 800-14 Generally Accepted Principles for Securing Information Technology Systems
 - SP 800-12 An Introduction to Computer Security: The NIST Handbook

TABLE 5-2 Elements of a Security Program

Primary Element	Components
Policy	Program Policy, Issue-Specific Policy, System-Specific Policy
Program Management	Central Security Program, System-Level Program
Risk Management	Risk Assessment, Risk Mitigation, Uncertainty Analysis
Life-Cycle Planning	Security Plan, Initiation Phase, Development/Acquisition Phase, Implementation Phase, Operation/Maintenance Phase
Personnel/User Issues	Staffing, User Administration
Preparing for Contingencies and Disasters	Business Plan, Identify Resources, Develop Scenarios, Develop Strategies, Test and Revise Plan
Computer Security Incident Handling	Incident Detection, Reaction, Recovery, and Followup
Awareness and Training	SETA plans, Awareness Projects, and Policy and Procedure Training
Security Considerations in Computer Support and Operations	Help Desk Integration, Defending Against Social Engineering, and Improving System Administration
Physical and Environmental Security	Guards, Gates, Locks and Keys, and Alarms
Identification and Authentication	Identification, Authentication, Passwords, Advanced Authentication
Logical Access Control	Access Criteria, Access Control Mechanisms
Audit Trails	System Logs, Log Review Processes, and Log Consolidation and Management
Cryptography	TKI, VPN, Key Management, and Key Recovery



Information Security Roles

- Information security positions can be classified into one of three types:
 - Those that define,
 - *provide the policies, guidelines, and standards. They're the people who do the consulting and the risk assessment, who develop the product and technical architectures. These are senior people with a lot of broad knowledge, but often not a lot of depth.*
 - Those that build
 - *They're the real techies, who create and install security solutions.*
 - Those that administer
 - *who operate and administrate the security tools, the security monitoring function, and the people who continuously improve the processes.*



Information Security Titles

- Typical organization has a number of individuals with information security responsibilities
- While the titles used may be different, most of the job functions fit into one of the following:
 - Chief Information Security Officer (CISO)
 - Security managers
 - Security administrators and analysts
 - Security technicians
 - Security staff

Information Security Roles

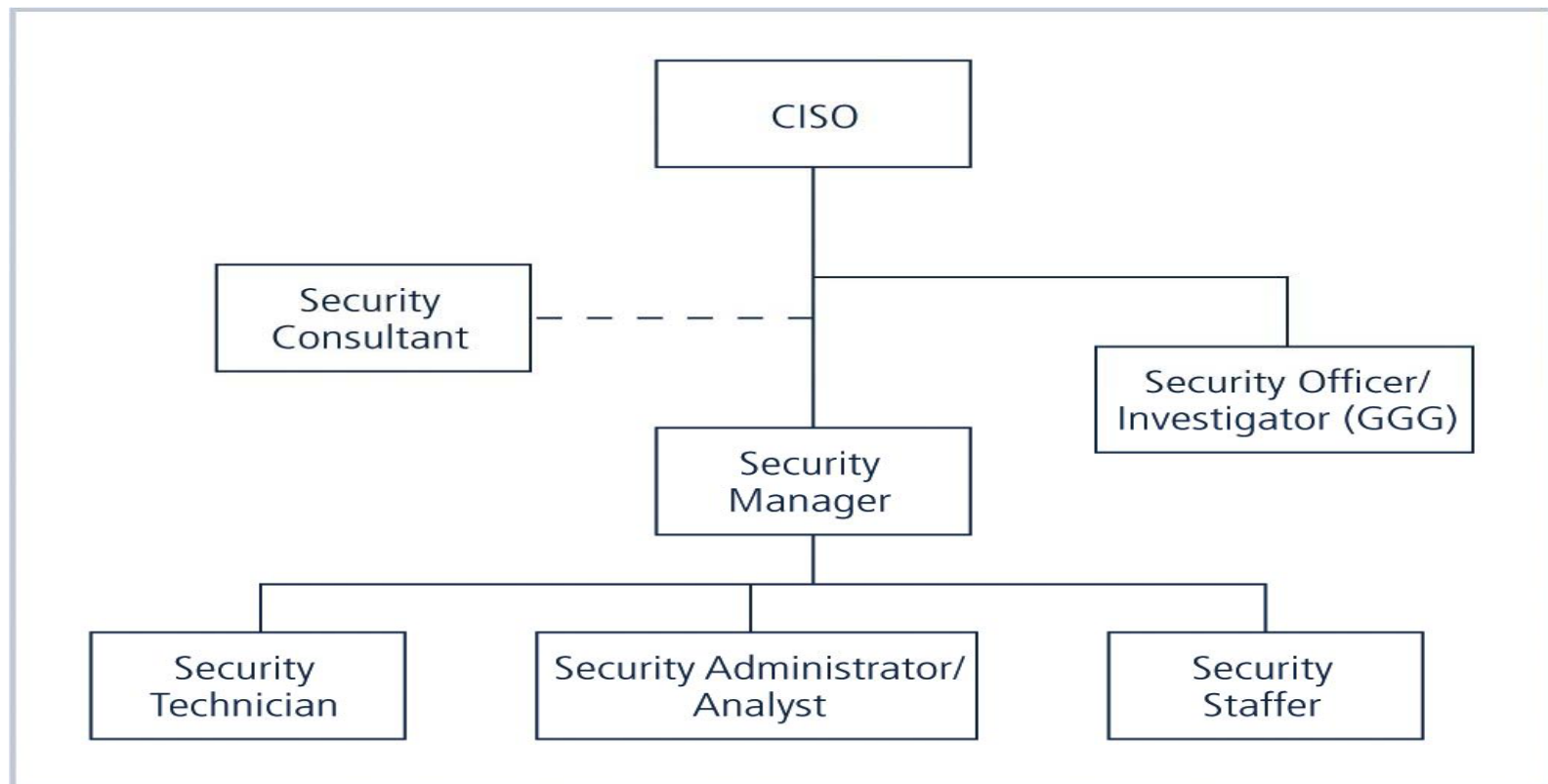


FIGURE 5-11 Information Security Roles



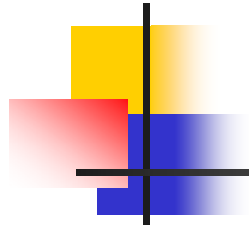
Integrating Security and the Help Desk

- Help desk
 - an important part of the information security team,
 - enhances the ability to identify potential problems
- User's complaint about his or her computer,
 - may turn out to be related to a bigger problem, such as a hacker, denial-of-service attack, or a virus
- Because help desk technicians perform a specialized role in information security,
 - they have a need for specialized training



Implementing Security Education, Training, and Awareness Programs

- SETA program:
 - designed to reduce accidental security breaches
 - consists of three elements:
 - security education,
 - security training, and
 - security awareness
- Awareness, training, and education programs offer two major benefits:
 - Improve employee behavior
 - Enable organization to hold employees accountable for their actions



Implementing SETA (Continued)

- The purpose of SETA is to enhance security:
 - By building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems
 - By developing skills and knowledge so that computer users can perform their jobs while using IT systems more securely
 - By improving awareness of the need to protect system resources



Comparative SETA Framework

	AWARENESS	TRAINING	EDUCATION
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching Method:	<u>Media</u> - Videos -Newsletters -Posters, etc.	<u>Practical Instruction</u> - Lecture - Case study workshop - Hands-on practice	<u>Theoretical Instruction</u> - Discussion Seminar - Background reading
Test Measure:	True/False Multiple Choice (identify learning)	Problem Solving (apply learning)	Eassay (interpret learning)
Impact Timeframe:	Short-term	Intermediate	Long-term



Security Training

- Security training involves
 - providing detailed information and
 - hands-on instruction to give skills to users to perform their duties securely
- Two methods for customizing training
 - Functional background:
 - General user
 - Managerial user
 - Technical user
 - Skill level:
 - Novice
 - Intermediate
 - Advanced



Training Techniques

- Using wrong method can:
 - Hinder transfer of knowledge
 - Lead to unnecessary expense and frustrated, poorly trained employees
- Good training programs:
 - Use latest learning technologies and best practices
 - Recently, less use of centralized public courses and more on-site training
 - Often for one or a few individuals, not necessarily for large group → waiting for large-enough group can cost companies productivity
 - Increased use of short, task-oriented modules and training sessions that are immediate and consistent, available during normal work week



Delivery Methods

- Selection of training delivery method:
 - Not always based on best outcome for the trainee
 - Other factors: budget, scheduling, and needs of the organization often come first
 - One-on-One
 - Formal Class
 - Computer-Based Training (CBT)
 - Distance Learning/Web Seminars
 - User Support Group
 - On-the-Job Training
 - Self-Study (Noncomputerized)



Selecting the Training Staff

- Employee training:
 - Local training program
 - Continuing education department
 - External training agency
 - Professional trainer, consultant, or someone from accredited institution to conduct on-site training
 - In-house training using organization's own employees



Implementing Training

- The following seven-step methodology generally applies:
 - Step 1: Identify program scope, goals, and objectives
 - Step 2: Identify training staff
 - Step 3: Identify target audiences
 - Step 4: Motivate management and employees
 - Step 5: Administer the program
 - Step 6: Maintain the program
 - Step 7: Evaluate the program



Security Awareness

- Security awareness program:
 - one of least frequently implemented, but most effective security methods
- Security awareness programs:
 - Set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure
 - Remind users of the procedures to be followed



SETA Best Practices

- When developing an awareness program:
 - Focus on people
 - Refrain from using technical jargon
 - Use every available venue
 - Define learning objectives, state them clearly, and provide sufficient detail and coverage
 - Keep things light
 - Don't overload the users
 - Help users understand their roles in InfoSec
 - Take advantage of in-house communications media
 - Make the awareness program formal; plan and document all actions
 - Provide good information early, rather than perfect information late



The Ten Commandments of InfoSec Awareness Training

- Information security is a people, rather than a technical, issue
- If you want them to understand, speak their language
- If they cannot see it, they will not learn it
- Make your point so that you can identify it and so can they
- Never lose your sense of humor
- Make your point, support it, and conclude it
- Always let the recipients know how the behavior that you request will affect them
- Ride the tame horses
- Formalize your training methodology
- Always be timely, even if it means slipping schedules to include urgent information



Employee Behavior and Awareness

- Security awareness and security training are designed to
 - modify any employee behavior that endangers the security of the organization's information
- Security training and awareness activities can be undermined
 - if management does not set a good example



Awareness Techniques

- Awareness can take on different forms for particular audiences
- A security awareness program can use many methods to deliver its message
- Effective security awareness programs need to be designed with the recognition that people tend to practice a tuning out process (acclimation)
 - Awareness techniques should be creative and frequently changed



Developing Security Awareness Components

- Many security awareness components are available at little or no cost - others can be very expensive if purchased externally
- Security awareness components include the following:
 - Videos
 - Posters and banners
 - Lectures and conferences
 - Computer-based training
 - Newsletters
 - Brochures and flyers
 - Trinkets (coffee cups, pens, pencils, T-shirts)
 - Bulletin boards



The Security Newsletter

- Security newsletter: cost-effective way to disseminate security information
 - In the form of hard copy, e-mail, or intranet
 - Topics can include threats to the organization's information assets, schedules for upcoming security classes, and the addition of new security personnel
- Goal:
 - keep information security uppermost in users' minds and stimulate them to care about security



The Security Newsletter (Continued)

- Newsletters might include:
 - Summaries of key policies
 - Summaries of key news articles
 - A calendar of security events, including training sessions, presentations, and other activities
 - Announcements relevant to information security
 - How-to's

The Security Poster

- Security poster series can be a simple and inexpensive way to keep security on people's minds
- Professional posters can be quite expensive, so in-house development may be best solution
- Keys to a good poster series:
 - Varying the content and keeping posters updated
 - Keeping them simple, but visually interesting
 - Making the message clear
 - Providing information on reporting violations



FIGURE 5-15 SETA Awareness Components: Posters

The Trinket Program

- Trinkets may not cost much on a per-unit basis, but they can be expensive to distribute throughout an organization
- Several types of trinkets are commonly used:
 - Pens and pencils
 - Mouse pads
 - Coffee mugs
 - Plastic cups
 - Hats
 - T-shirts



FIGURE 5-16 SETA Awareness Components: Trinkets



Information Security Awareness Web Site

- Organizations can establish
 - Web pages or sites dedicated to promoting information security awareness
- As with other SETA awareness methods,
 - the challenge lies in updating the messages frequently enough to keep them fresh



Information Security Awareness Web Site (Continued)

- Some tips on creating and maintaining an educational Web site are provided here:
 - See what's already out there
 - Plan ahead
 - Keep page loading time to a minimum
 - Seek feedback
 - Assume nothing and check everything
 - Spend time promoting your site



Security Awareness Conference/Presentations

- Another means of renewing the information security message is to have a guest speaker or even a mini-conference dedicated to the topic
 - Perhaps in association with National Computer Security Day - November 30

