

Review of Information Security

By Kouros

What is Security? (cont'd.)

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle
 - Was standard based on confidentiality, integrity, and availability
 - Now expanded into list of critical characteristics of information

Introduction

- Information security: a “well-informed sense of assurance that the information risks and controls are in balance.”
- Security professionals must review the origins of this field to understand its impact on our understanding of information security today

CNSS Security Model

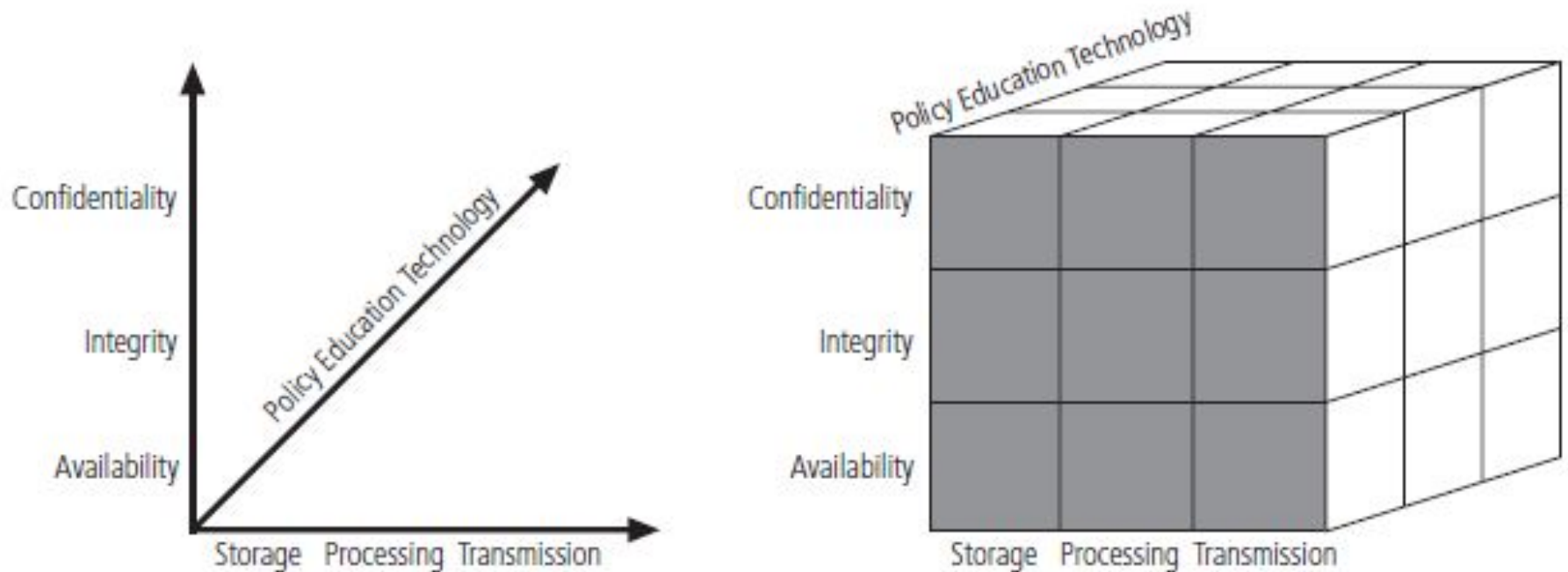


Figure 1-6 The McCumber Cube

Desired goal, Information STATE, safeguard

Components of an Information System

- Information system (IS) is entire set of components necessary to use information as a resource in the organization
 - Software
 - Hardware
 - Data
 - People
 - Procedures
 - Networks

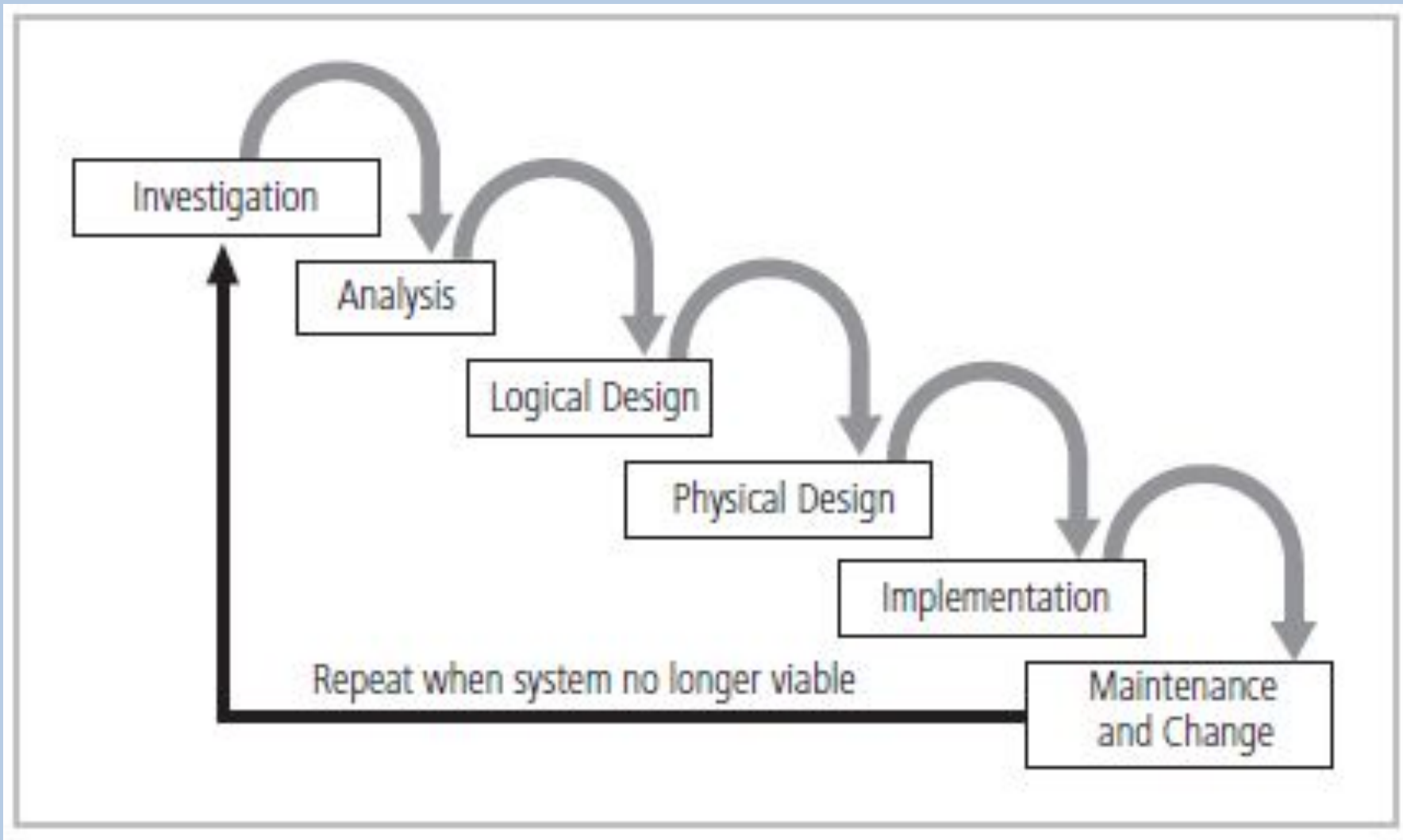


Figure 1-10 SDLC Waterfall Methodology (life cycle)

Analysis

- Documents from investigation phase are studied
- Analysis of existing security policies or programs, along with documented current threats and associated controls
- Includes analysis of relevant **legal issues** that could impact design of the security solution
- **Risk management task begins**

Implementation

- **Security solutions are acquired, tested, implemented, and tested again**
- Personnel issues evaluated; specific **training and education** programs conducted
- Entire tested package is presented to management for final approval

Summary

- Information security is a “well-informed sense of assurance that the information risks and controls are in balance”
- Computer security began immediately after first mainframes were developed
- Successful organizations have multiple layers of security in place: physical, personal, operations, communications, network, and information
- Security should be considered a balance between protection and availability
- Information security must be managed similarly to any major system implemented in an organization using a methodology like Security SDLC

EVERYTHING NEEDS A BREAK.

Threats

- Threat: an object, person, or other entity that represents a constant danger to an asset
- Management must be informed of the different threats facing the organization
- Overall security is improving

	Category of Threat	Examples
1.	Compromises to intellectual property	Piracy, copyright infringement
2.	Software attacks	Viruses, worms, macros, denial of service
3.	Deviations in quality of service	ISP, power, or WAN service issues from service providers
4.	Espionage or trespass	Unauthorized access and/or data collection
5.	Forces of nature	Fire, flood, earthquake, lightning
6.	Human error or failure	Accidents, employee mistakes
7.	Information extortion	Blackmail, information disclosure
8.	Missing, inadequate, or incomplete	Loss of access to information systems due to disk in place drive failure without proper backup and recovery plan organizational policy or planning
9.	Missing, inadequate, or incomplete controls	Network compromised because no firewall security controls
10.	Sabotage or vandalism	Destruction of systems or information
11.	Theft	Illegal confiscation of equipment or information
12.	Technical hardware failures or errors	Equipment failure
13.	Technical software failures or errors	Bugs, code problems, unknown loopholes
14.	Technological obsolescence	Antiquated or outdated technologies

Table 2-1 Threats to Information Security⁴

Deliberate Software Attacks

- Malicious software (malware) designed to damage, destroy, or deny service to target systems
- Includes:
 - Viruses
 - Worms
 - Trojan horses
 - Logic bombs
 - Back door or trap door
 - Polymorphic threats
 - Virus and worm hoaxes

More about previous slide

- **Deliberate Software Attacks**
- Deliberate software attacks occur when an individual or group designs software to attack an unsuspecting system. Most of this software is referred to as malicious code or malicious software, or sometimes malware.
- These software components or programs are designed to damage, destroy, or deny service to the target systems.
- Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic bombs, back doors, and denial-of-services attacks.
- Computer viruses are segments of code that perform malicious actions.
- This code behaves very much like a virus pathogen attacking animals and plants, using the cell's own replication machinery to propagate and attack.
- The code attaches itself to the existing program and takes control of that program's access to the targeted computer.
- The virus-controlled target program then carries out the virus's plan by replicating itself into additional targeted systems.
- The macro virus is embedded in the automatically executing macro code, common in office productivity software like word processors, spread sheets, and database applications.
- The boot virus infects the key operating systems files located in a computer's boot sector.
- Worms - Malicious programs that replicate themselves constantly without requiring another program to provide a safe environment for replication. Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.
- Trojan horses - Software programs that hide their true nature and reveal their designed behavior only when activated. Trojan horses are frequently disguised as helpful, interesting, or necessary pieces of software, such as readme.exe files often included with shareware or freeware packages.
- Back door or Trap door - A virus or worm can have a payload that installs a back door or trap door component in a system. This allows the attacker to access the system at will with special privileges.
- Polymorphism - A threat that changes its apparent shape over time, representing a new threat not detectable by techniques that are looking for a preconfigured signature. These threats actually evolve, changing their size and appearance to elude detection by antivirus software programs, making detection more of a challenge.
- Virus and Worm Hoaxes - As frustrating as viruses and worms are, perhaps more time and money is spent on resolving virus hoaxes. Well-meaning people spread the viruses and worms when they send e-mails warning of fictitious or virus laden threats.

Espionage or Trespass (cont'd.)

- Expert hacker
 - Develops software scripts and program exploits
 - Usually a master of many skills
 - Will often create attack software and share with others
- Unskilled hacker
 - Many more unskilled hackers than expert hackers
 - Use expertly written software to exploit a system
 - Do not usually fully understand the systems they hack

Attacks

- Attacks
 - Acts or actions that exploits vulnerability (i.e., an identified weakness) in controlled system
 - Accomplished by threat agent that damages or steals organization's information
- Types of attacks
 - Malicious code: includes execution of viruses, worms, Trojan horses, and active Web scripts with intent to destroy or steal information
 - Hoaxes: transmission of a virus hoax with a real virus attached; more devious form of attack

Attacks (cont'd.)

- Types of attacks (cont'd.)
 - Back door: gaining access to system or network using known or previously unknown/newly discovered access mechanism
 - Password crack: attempting to reverse calculate a password
 - Brute force: trying every possible combination of options of a password
 - Dictionary: selects specific accounts to attack and uses commonly used passwords (i.e., the dictionary) to guide guesses

Attacks (cont'd.)

- Types of attacks (cont'd.)
 - Denial-of-service (DoS): attacker sends large number of connection or information requests to a target
 - Target system cannot handle successfully along with other, legitimate service requests
 - May result in system crash or inability to perform ordinary functions
 - Distributed denial-of-service (DDoS): coordinated stream of requests is launched against target from many locations simultaneously

Attacks (cont'd.)

- Types of attacks (cont'd.)
 - Spoofing: technique used to gain unauthorized access; intruder assumes a trusted IP address
 - Man-in-the-middle: attacker monitors network packets, modifies them, and inserts them back into network
 - Spam: unsolicited commercial e-mail; more a nuisance than an attack, though is emerging as a vector for some attacks
 - Mail bombing: also a DoS; attacker routes large quantities of e-mail to target

Attacks (cont'd.)

- Types of attacks (cont'd.)
 - Sniffers: program or device that monitors data traveling over network; can be used both for legitimate purposes and for stealing information from a network
 - Phishing: an attempt to gain personal/financial information from individual, usually by posing as legitimate entity
 - Pharming: redirection of legitimate Web traffic (e.g., browser requests) to illegitimate site for the purpose of obtaining private information

Attacks (cont'd.)

- Types of attacks (cont'd.)
 - Social engineering: using social skills to convince people to reveal access credentials or other valuable information to attacker
 - “People are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything.” — Kevin Mitnick
 - Timing attack: relatively new; works by exploring contents of a Web browser's cache to create malicious cookie

TAKE A DEEP BREATH

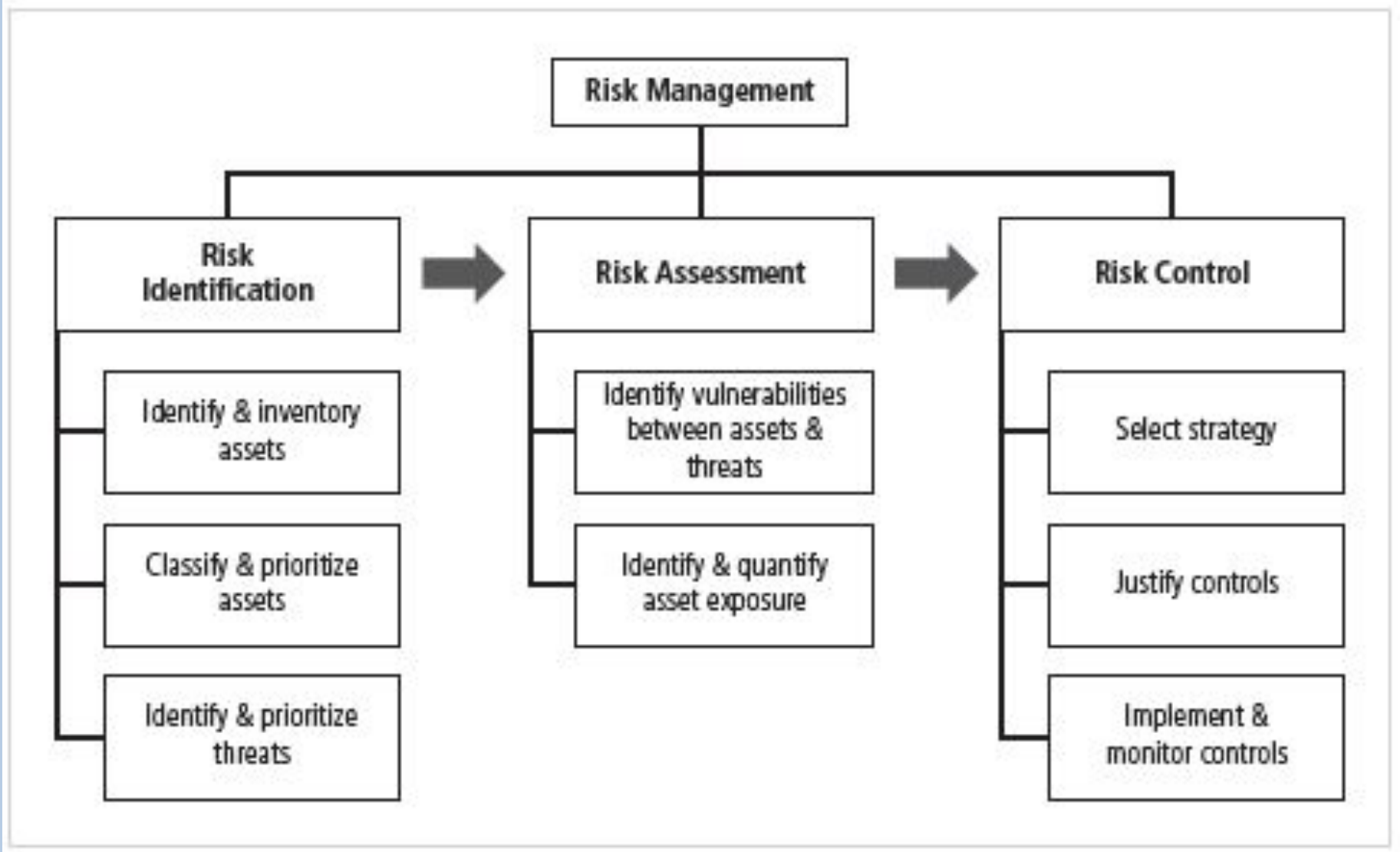


Figure 4-1 Components of Risk Management

Risk Identification

- Risk management involves identifying, classifying, and prioritizing an organization's assets
- A threat assessment process identifies and quantifies the risks facing each asset
- Components of risk identification
 - People
 - Procedures
 - Data
 - Software
 - Hardware

Risk Assessment

- Risk assessment evaluates the relative risk for each vulnerability
- Assigns a risk rating or score to each information asset
- The goal at this point: create a method for evaluating the relative risk of each listed vulnerability

Deliverable

Purpose

Information asset classification worksheet	Assembles information about information assets and their impact
Weighted criteria analysis worksheet	Assigns ranked value or impact weight to each information asset
Ranked vulnerability risk worksheet	Assigns ranked value of risk rating for each uncontrolled asset-vulnerability pair

Table 4-10 Risk Identification and Assessment Deliverables

Access Control

- Access control: method by which systems determine whether and how to admit a user into a trusted area of the organization
- Mandatory access controls (MACs): use data classification schemes
- Nondiscretionary controls: strictly-enforced version of MACs that are managed by a central authority
- Discretionary access controls (DACs): implemented at the discretion or option of the data user

Identification

- **Identification:** mechanism whereby an unverified entity that seeks access to a resource proposes a label by which they are known to the system
- **Identifiers** can be composite identifiers, concatenating elements-department codes, random numbers, or special characters to make them unique

Authentication

- Authentication: the process of validating a supplicant's purported identity
- Authentication factors
 - Something a supplicant knows
 - Password: a private word or combination of characters that only the user should know
 - Passphrase: a series of characters, typically longer than a password, from which a virtual password is derived
 - Something a supplicant has
 - Smart card: contains a computer chip that can verify and validate information
 - Synchronous and Asynchronous tokens
 - Something a supplicant is
 - Relies upon individual characteristics
 - Strong authentication

Authorization

- Authorization: the matching of an authenticated entity to a list of information assets and corresponding access levels

TAKE A REST

Firewalls Processing Modes

- Five processing modes by which firewalls can be categorized:
 - Packet filtering
 - Application gateways
 - Circuit gateways
 - MAC layer firewalls
 - Hybrids(combination of other methods)

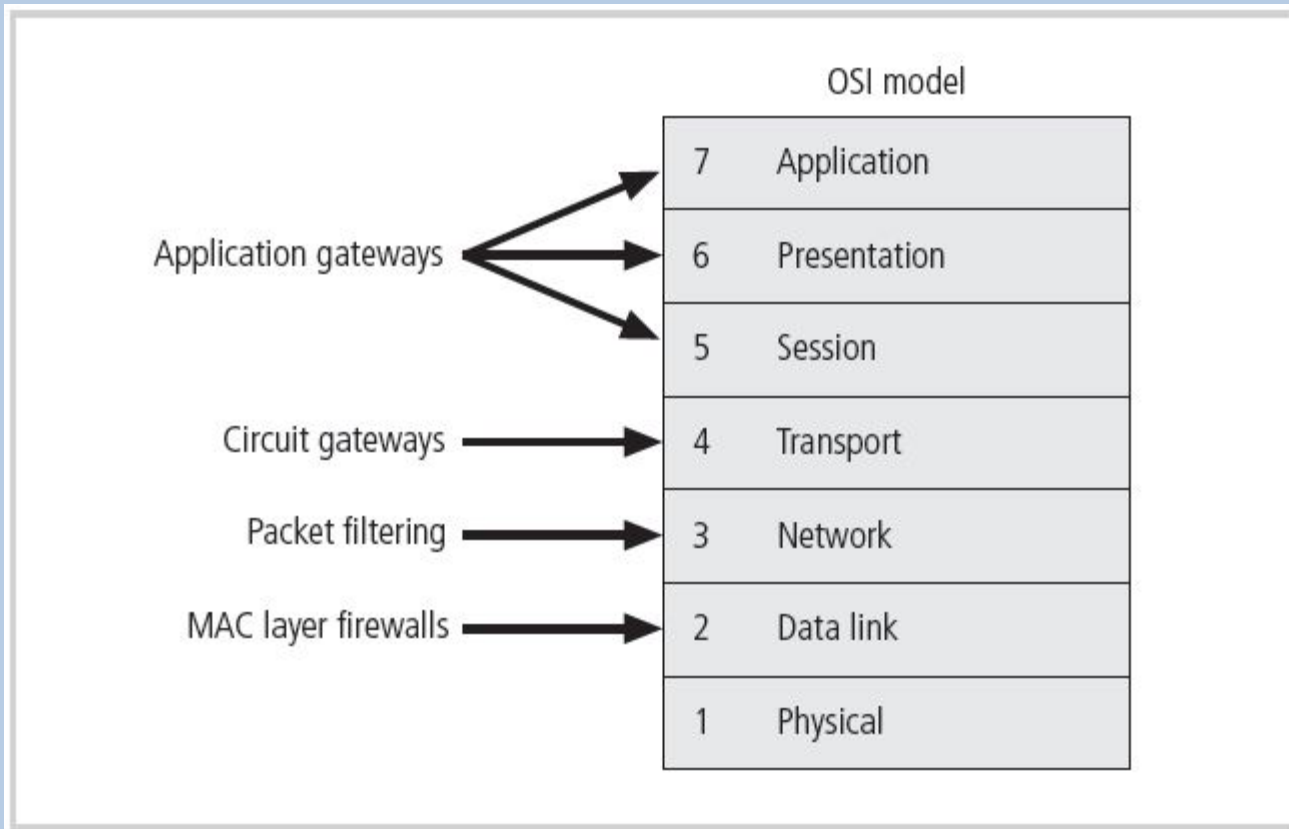


Figure 6-6 Firewall Types and the OSI Model

Firewall Architectures (cont'd.)

- **Dual-homed host firewalls**
 - Bastion host contains two network interface cards (NICs): one connected to external network, one connected to internal network
 - Implementation of this architecture often makes use of network address translation (NAT), creating another barrier to intrusion from external attackers

Firewalls Processing Modes (cont'd.)

- **Application gateways**
 - Frequently installed on a dedicated computer; also known as a **proxy server**
 - Since proxy server is often placed in unsecured area of the network (e.g., DMZ), it is exposed to higher levels of risk from less trusted networks
 - Additional filtering routers can be implemented behind the proxy server, further protecting internal systems

Virtual Private Networks (VPNs)

- Private and secure network connection between systems; uses data communication capability of unsecured and public network
- Securely extends organization's internal network connections to remote locations beyond trusted network

Intrusion Detection and Prevention Systems (cont'd.)

- **Intrusion detection:** consists of **procedures and systems** created and operated to **detect** system intrusions
- **Intrusion reaction:** encompasses **actions** an organization **undertakes** when intrusion event is detected
- **Intrusion correction** activities: finalize restoration of operations to a normal state

Honeypots, Honeynets, and Padded Cell Systems

- **Honeypots:** decoy systems designed to lure potential attackers away from critical systems and encourage attacks against the themselves
- **Honeynets:** collection of honeypots connecting several honey pot systems on a subnet
- Honeypots designed to:
 - **Divert attacker from accessing critical systems**
 - **Collect information about attacker's activity**
 - **Encourage attacker to stay on system long enough for administrators to document event and, perhaps, respond**

Firewall Analysis Tools

- Several tools automate remote discovery of firewall rules and assist the administrator in analyzing them
- Administrators who feel wary of using the same tools that attackers use should remember:
 - It is intent of user that will dictate how information gathered will be used
 - In order to defend a computer or network well, it is necessary to understand ways it can be attacked
- A tool that can help close up an open or poorly configured firewall will help network defender minimize risk from attack

Scanning and Analysis Tools

- Typically used to collect information that attacker would need to launch successful attack
- **Attack protocol** is series of steps or processes used by an attacker, in a logical sequence, to launch attack against a target system or network
- **Footprinting**: the organized research of Internet addresses owned or controlled by a target organization

Scanning and Analysis Tools (cont'd.)

- **Fingerprinting:** systematic survey of all of target organization's Internet addresses collected during the footprinting phase
- **Fingerprinting** reveals useful information about internal structure and operational nature of target system or network for anticipated attack
- These tools are valuable to network defender since they can quickly pinpoint the parts of the systems or network that need a prompt repair to close the vulnerability

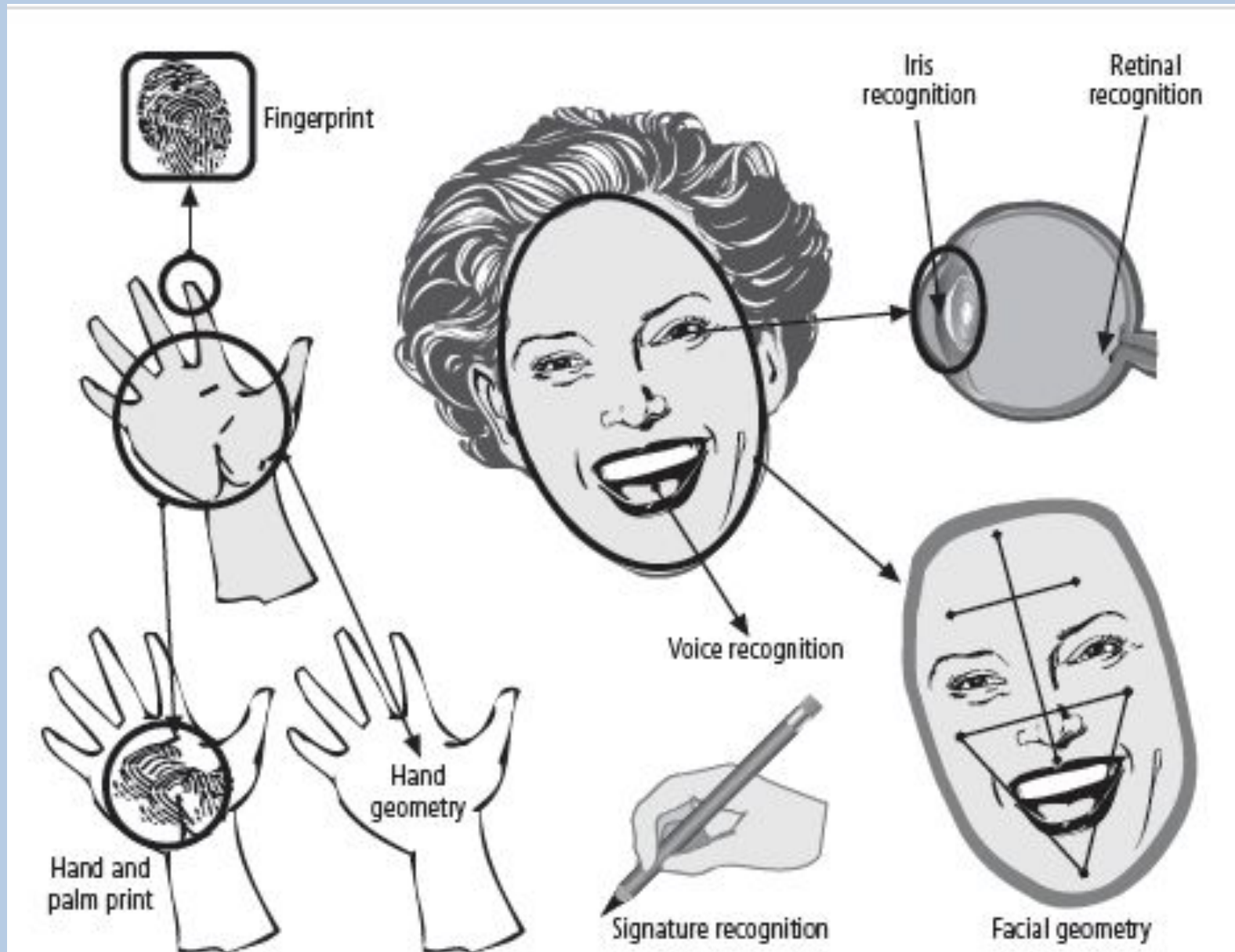



Figure 7-20 Biometric Recognition Characteristics

HAVE SOME REST

- 
- **Cryptology:** science of encryption; combines cryptography and cryptanalysis
 - **Cryptography:** process of making and using codes to secure transmission of information
 - **Cryptanalysis:** process of obtaining original message from encrypted message without knowing algorithms
 - **Encryption:** converting original message into a form unreadable by unauthorized individuals
 - **Decryption:** the process of converting the ciphertext message back into plaintext

Substitution Cipher

- Substitute one value for another
- Monoalphabetic substitution: uses only one alphabet
- Polyalphabetic substitution: more advanced; uses two or more alphabets
- Vigenère cipher: advanced cipher type that uses simple polyalphabetic code; made up of 26 distinct cipher alphabets

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Table 8-2 The Vigenère Square

Cryptographic Algorithms

- Often grouped into two broad categories, symmetric and asymmetric
 - Today's popular cryptosystems use hybrid combination of symmetric and asymmetric algorithms
- Symmetric and asymmetric algorithms distinguished by types of keys used for encryption and decryption operations

Symmetric Encryption (cont'd.)

- Data Encryption Standard (DES): one of most popular symmetric encryption cryptosystems
 - 64-bit block size; 56-bit key
 - Adopted by NIST in 1976 as federal standard for encrypting non-classified information
- Triple DES (3DES): created to provide security far beyond DES
- Advanced Encryption Standard (AES): developed to replace both DES and 3DES

Asymmetric Encryption

- Also known as public-key encryption
- Uses two different but related keys
 - Either key can encrypt or decrypt message
 - If Key A encrypts message, only Key B can decrypt
 - Highest value when one key serves as private key and the other serves as public key
- RSA algorithm

Asymmetric Encryption

- Also known as public-key encryption
- Uses two different but related keys
 - Either key can encrypt or decrypt message
 - If Key A encrypts message, only Key B can decrypt
 - Highest value when one key serves as private key and the other serves as public key
- RSA algorithm

Symmetric Encryption (cont'd.)

- Data Encryption Standard (DES): one of most popular symmetric encryption cryptosystems
 - 64-bit block size; 56-bit key
 - Adopted by NIST in 1976 as federal standard for encrypting non-classified information
- Triple DES (3DES): created to provide security far beyond DES
- Advanced Encryption Standard (AES): developed to replace both DES and 3DES

Symmetric Encryption

- Uses same “secret key” to encipher and decipher message
 - Encryption methods can be extremely efficient, requiring minimal processing
 - Both sender and receiver must possess encryption key
 - If either copy of key is compromised, an intermediate can decrypt and read messages

Securing Internet Communication with S-HTTP and SSL

- Secure Socket Layer (SSL) protocol: uses public key encryption to secure channel over public Internet
- Secure Hypertext Transfer Protocol (S-HTTP): extended version of Hypertext Transfer Protocol; provides for encryption of individual messages between client and server across Internet
- S-HTTP is the application of SSL over HTTP
 - Allows encryption of information passing between computers through protected and secure virtual connection

Securing e-mail with S/MIME, PEM, and PGP

- Secure Multipurpose Internet Mail Extensions (S/MIME): builds on Multipurpose Internet Mail Extensions (MIME) encoding format by adding encryption and authentication
- Privacy Enhanced Mail (PEM): proposed as standard to function with public-key cryptosystems; uses 3DES symmetric key encryption
- Pretty Good Privacy (PGP): uses IDEA Cipher for message encoding

Securing Web transactions with SET, SSL, and S-HTTP

- Secure Electronic Transactions (SET): developed by MasterCard and VISA in 1997 to provide protection from electronic payment fraud
- Uses DES to encrypt credit card information transfers
- Provides security for both Internet-based credit card transactions and credit card swipe systems in retail stores

Securing Wireless Networks with WEP and WPA

- Wired Equivalent Privacy (WEP): early attempt to provide security with the 802.11 network protocol
- Wi-Fi Protected Access (WPA and WPA2): created to resolve issues with WEP
- Next Generation Wireless Protocols: Robust Secure Networks (RSN), AES – Counter Mode Encapsulation, AES – Offset Codebook Encapsulation
- Bluetooth: can be exploited by anyone within approximately 30 foot range, unless suitable security controls are implemented

Steganography

- Process of hiding information
- Has been in use for a long time
- Most popular modern version hides information within files appearing to contain digital pictures or other images
- Some applications hide messages in .bmp, .wav, .mp3, and .au files, as well as in unused space on CDs and DVDs

DO YOU WANT A CUP OF COFFEE?!

Introduction

- Physical security addresses design, implementation, and maintenance of countermeasures that protect physical resources of an organization
- Most controls can be circumvented if an attacker gains physical access
- Physical security is as important as logical security

Uninterruptible power supply (UPS)

- Uninterruptible power supply (UPS)
 - In case of power outage, UPS is backup power source for major computer systems
 - **Four basic UPS configurations:**
 - **Standby**
 - **Ferroresonant standby**
 - **Line-interactive**
 - **True online (double conversion online)**

Heating, Ventilation, and Air Conditioning

- Areas within heating, ventilation, and air conditioning (HVAC) systems that can cause damage to information systems include:
 - Temperature
 - Filtration
 - Humidity
 - Static electricity

Physical Security Controls (cont'd.)

- Electronic Monitoring
 - Records events where other types of physical controls are impractical or incomplete
 - May use cameras with video recorders; includes closed-circuit television (CCT) systems
 - Drawbacks
 - Reactive; does not prevent access or prohibited activity
 - Recordings often are not monitored in real time; must be reviewed to have any value

Summary

- Threats to information security that are unique to physical security
- Key physical security considerations in a facility site
- Physical security monitoring components
- Essential elements of access control
- Fire safety, fire detection, and response
- Importance of supporting utilities, especially use of uninterruptible power supplies
- Countermeasures to physical theft of computing devices

Introduction

- SecSDLC implementation phase is accomplished through changing configuration and operation of organization's information systems
- Implementation includes changes to:
 - **Procedures (through policy)**
 - **People (through training)**
 - **Hardware (through firewalls and intrusion detection system)**
 - **Software (through encryption)**
 - **Data (through classification)**
- Organization translates blueprint for information security into a concrete project plan

Developing the Project Plan

- Creation of project plan can be done using work breakdown structure (WBS)
- Major project tasks in WBS are:
 - Work to be accomplished
 - Assignees
 - Start and end dates
 - Amount of effort required
 - Estimated capital and noncapital expenses
 - Identification of dependencies between/among tasks
- Each major WBS task is further divided into smaller tasks or specific action steps

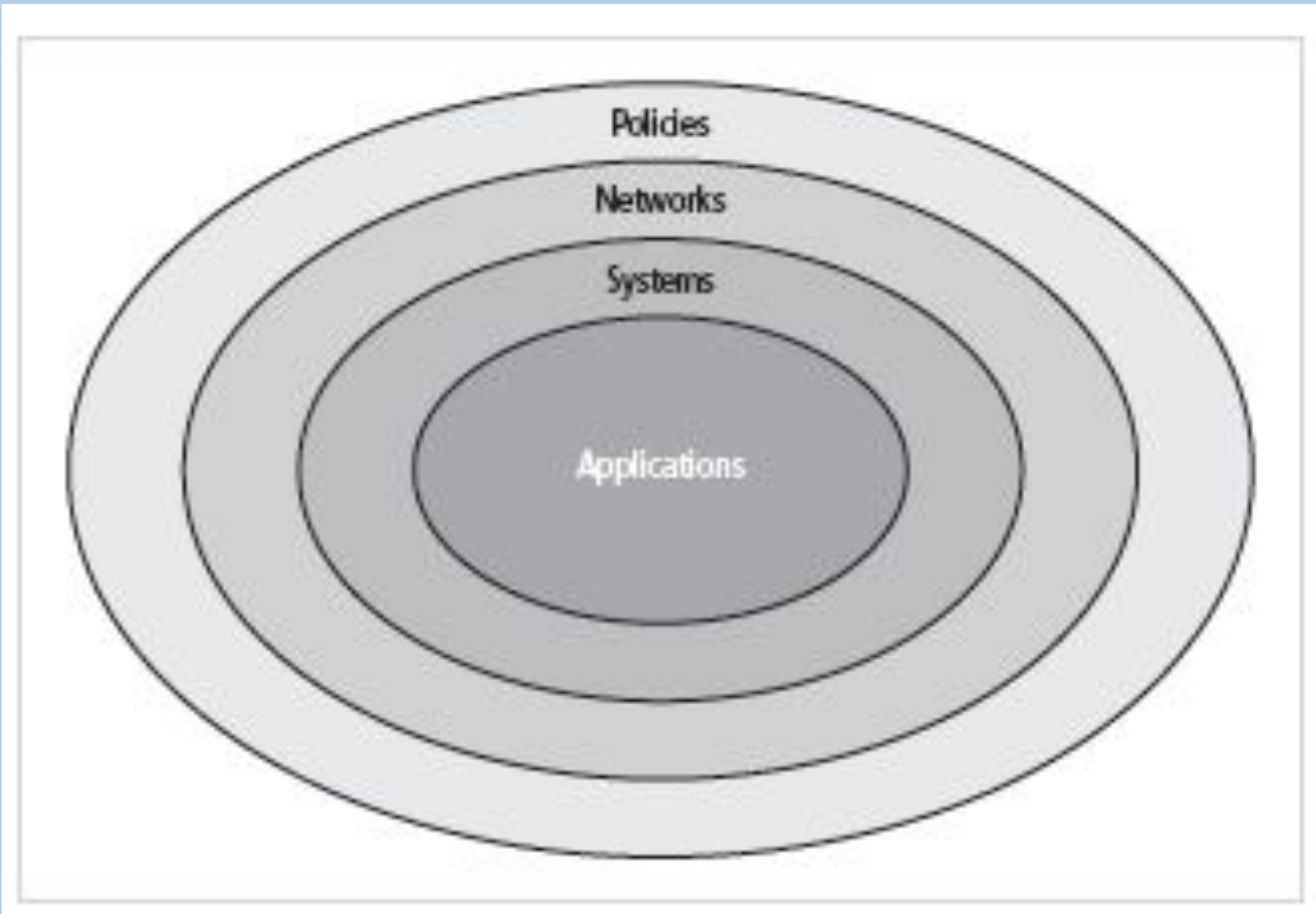


Figure 10-2 The Bull's-Eye Model

Positioning and Staffing the Security Function

- The security function can be placed within:
 - IT function
 - Physical security function
 - Administrative services function
 - Insurance and risk management function
 - Legal department
- Organizations balance needs of enforcement with needs for education, training, awareness, and customer service

Positioning and Staffing the Security Function

- The security function can be placed within:
 - IT function
 - Physical security function
 - Administrative services function
 - Insurance and risk management function
 - Legal department
- Organizations balance needs of enforcement with needs for education, training, awareness, and customer service

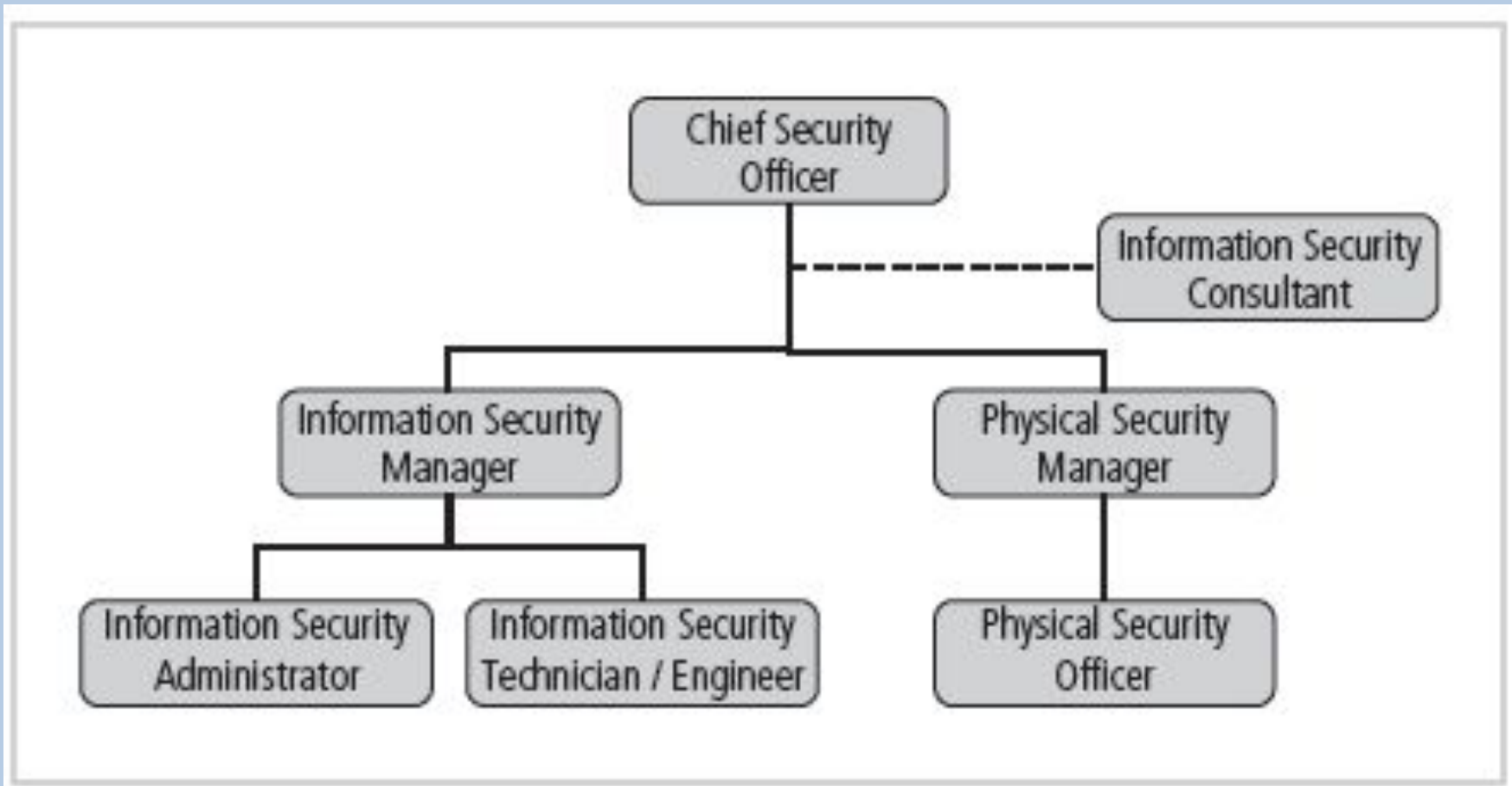


Figure 11-2 Positions in Information Security

Staffing the Information Security Function (cont'd.)

- Chief Information Security Officer (CISO or CSO)
 - Top information security position; frequently reports to Chief Information Officer (CIO)
 - Manages the overall information security program
 - Drafts or approves information security policies
 - Works with the CIO on strategic plans

Staffing the Information Security Function (cont'd.)

- Security manager
 - Accountable for day-to-day operation of information security program
 - Accomplish objectives as identified by CISO
 - Typical qualifications: not uncommon to have accreditation; ability to draft middle- and lower-level policies; standards and guidelines; budgeting, project management, and hiring and firing; manage technicians

Staffing the Information Security Function (cont'd.)

- Security technician
 - Technically qualified individuals tasked to configure security hardware and software
 - Tend to be specialized
 - Typical qualifications:
 - Varied; organizations prefer expert, certified, proficient technician
 - Some experience with a particular hardware and software package
 - Actual experience in using a technology usually required

**IT MIGHT BE A BAD DAY,
NOT A BAD LIFE**

The Security Maintenance Model

- Designed to focus organizational effort on maintaining systems
- Recommended maintenance model based on five subject areas:
 - External monitoring
 - Internal monitoring
 - Planning and risk assessment
 - Vulnerability assessment and remediation
 - Readiness and review

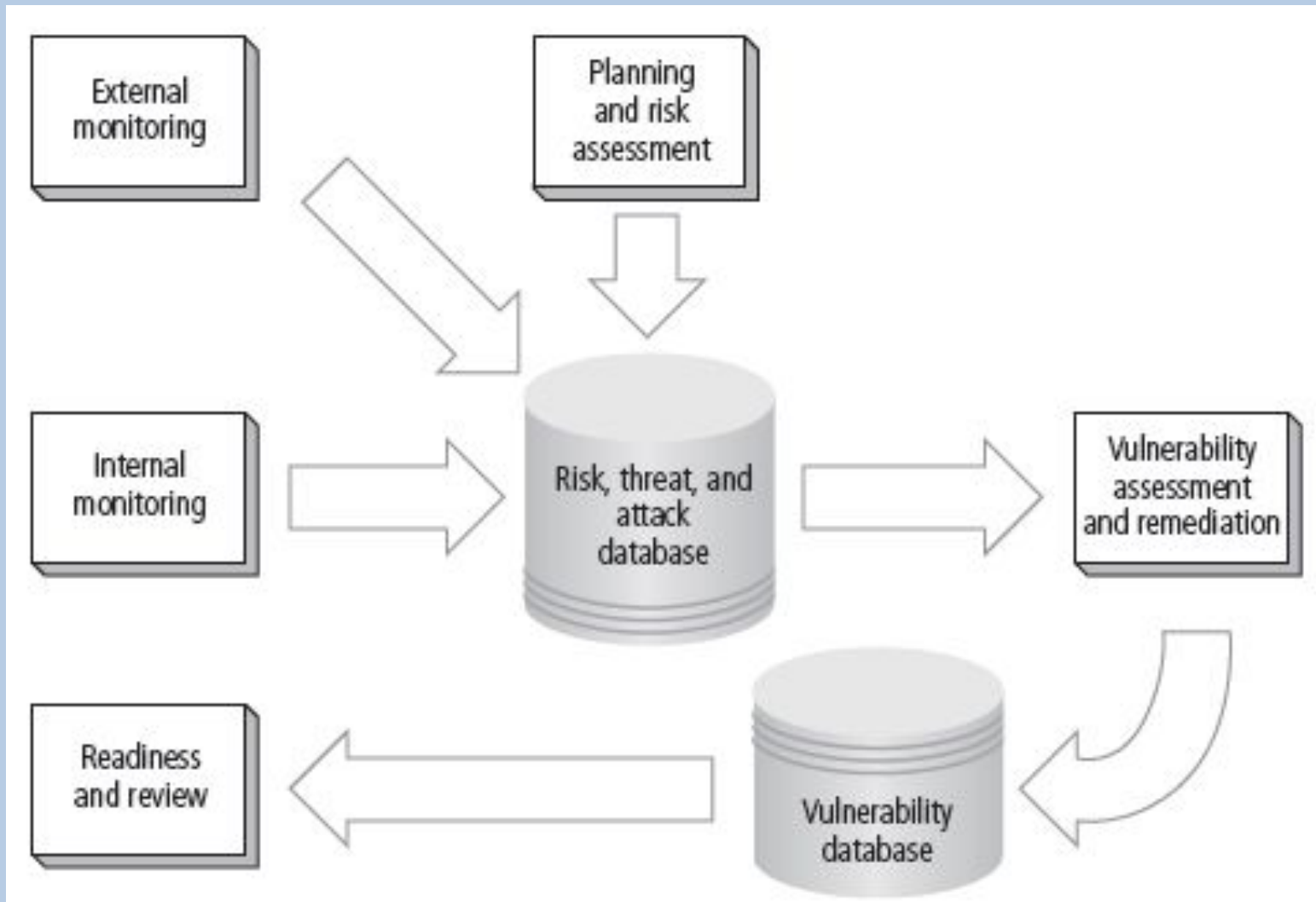


Figure 12-10 The Maintenance Model

Monitoring the External Environment

- Objective to provide early awareness of new threats, threat agents, vulnerabilities, and attacks that is needed to mount an effective defense
- Entails collecting intelligence from data sources and giving that intelligence context and meaning for use by organizational decision makers

Monitoring the Internal Environment

- Maintain informed awareness of state of organization's networks, systems, and security defenses
- Internal monitoring accomplished by:
 - Doing inventory of network devices and channels, IT infrastructure and applications, and information security infrastructure elements
 - Leading the IT governance process
 - Real-time monitoring of IT activity
 - Monitoring the internal state of the organization's networks and systems

Planning and Risk Assessment

- Primary objective is to keep lookout over entire information security program
- Accomplished by identifying and planning ongoing information security activities that further reduce risk

Vulnerability Assessment and Remediation

- Primary goal: identification of specific, documented vulnerabilities and their timely remediation
- Accomplished by:
 - Using vulnerability assessment procedures
 - Documenting background information and providing tested remediation procedures for vulnerabilities
 - Tracking vulnerabilities from when they are identified
 - Communicating vulnerability information to owners of vulnerable systems
 - Reporting on the status of vulnerabilities
 - Ensuring the proper level of management is involved

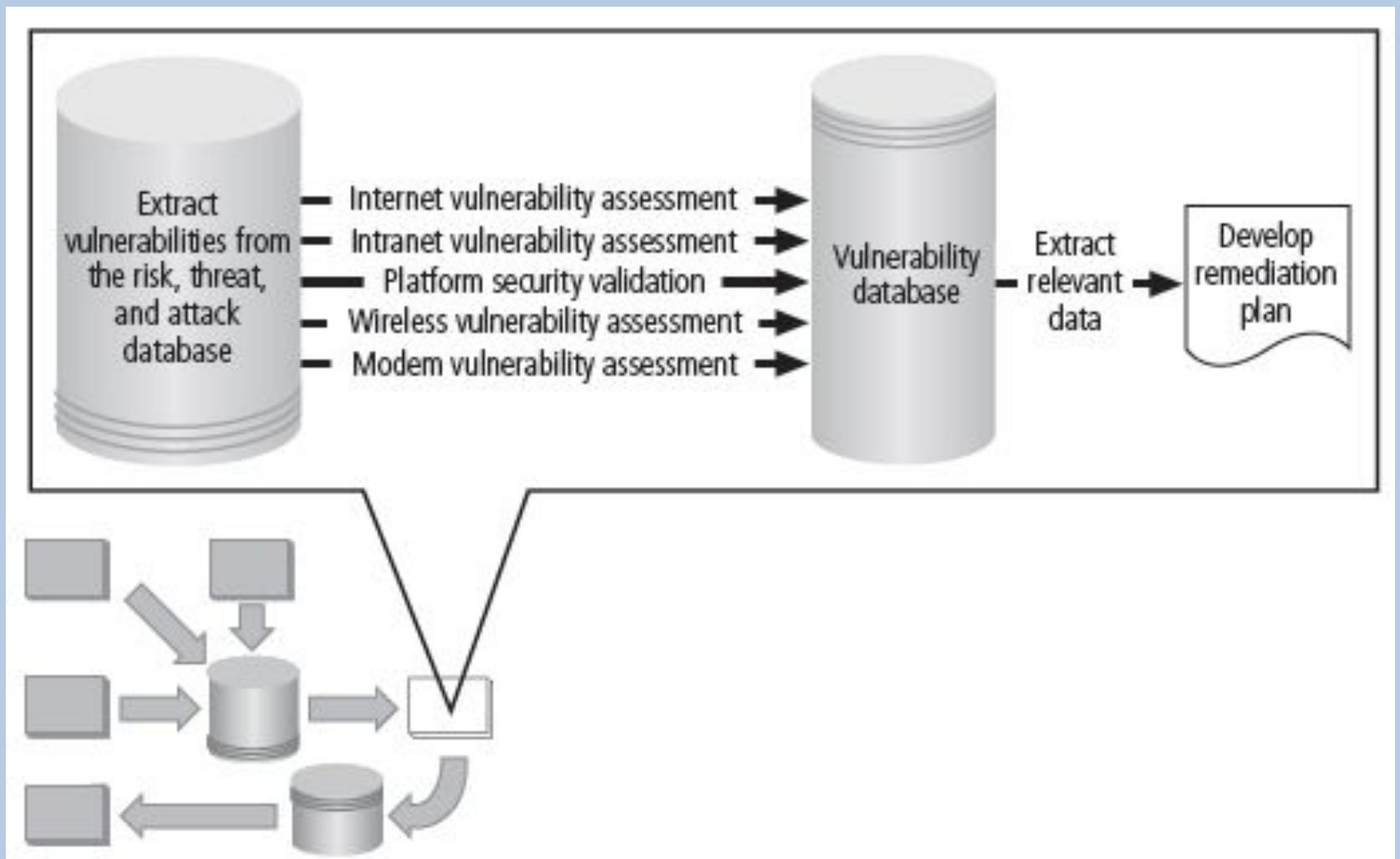


Figure 12-15 Vulnerability Assessment and Remediation

Definitions

- **Policy:** course of action used by organization to convey 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, read, understood, and agreed to by all members of organization and uniformly enforced

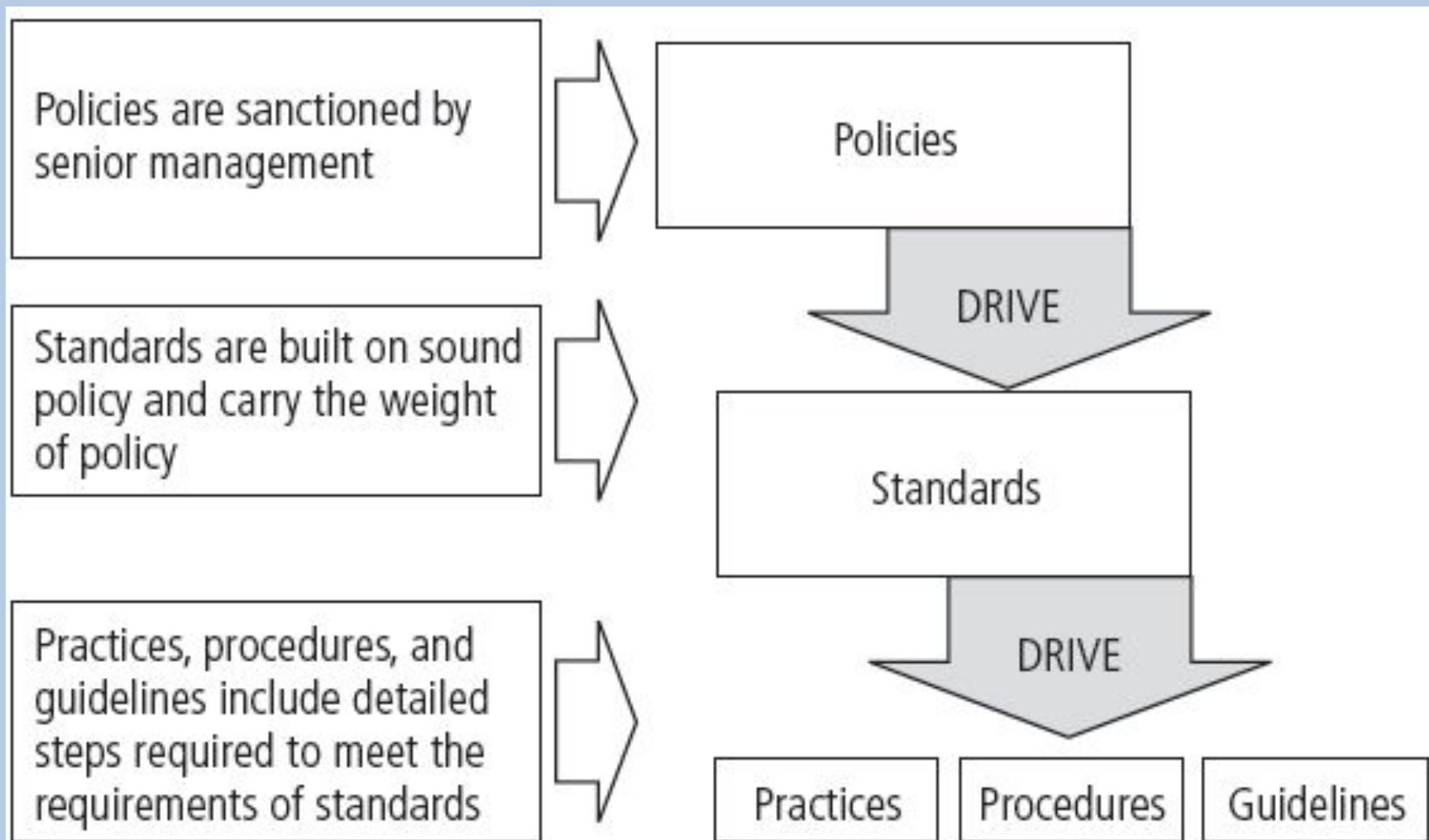


Figure 5-1 Policies, Standards, and Practices

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

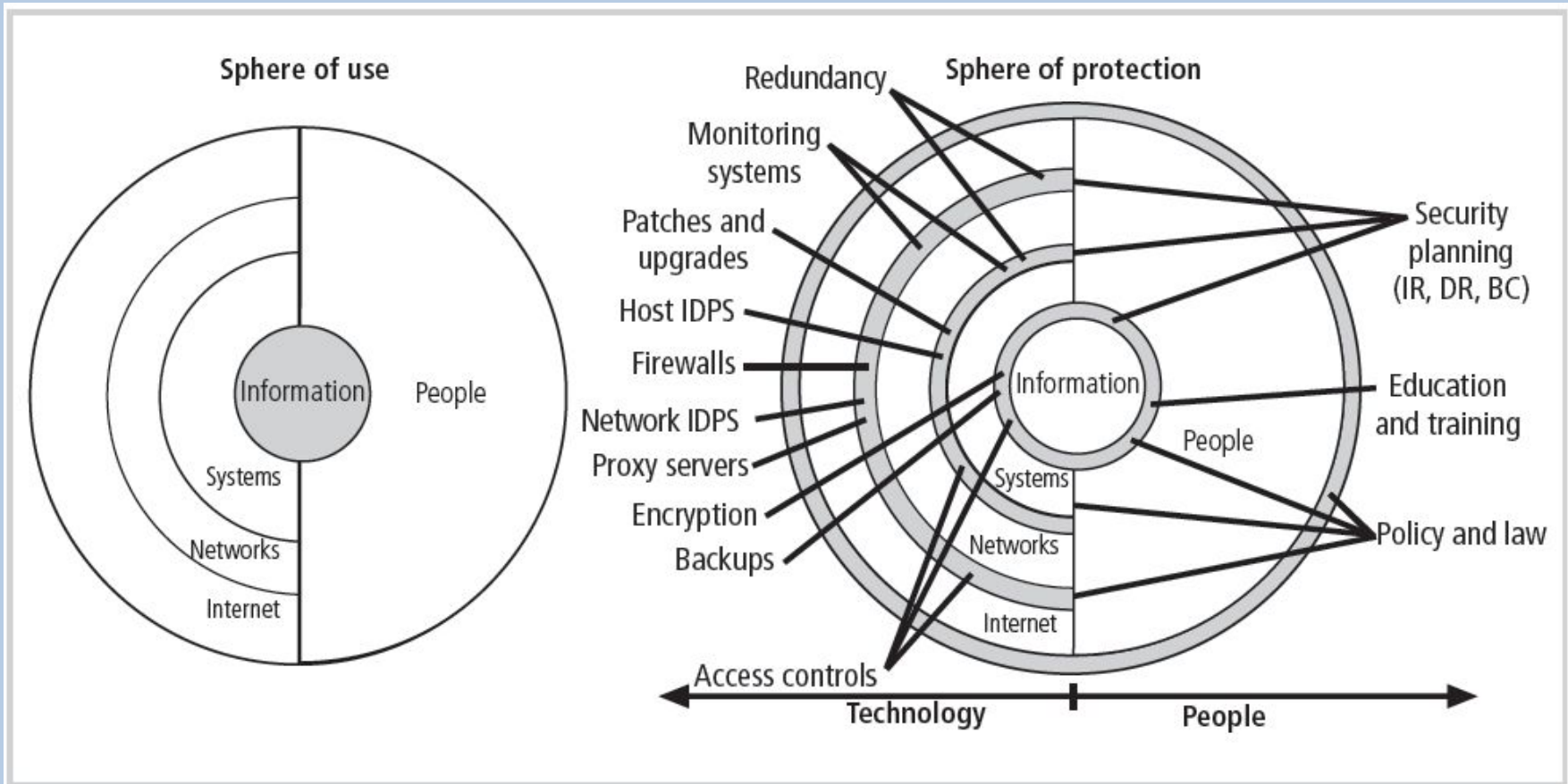


Figure 5-8 Spheres of Security

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: a server that 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

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

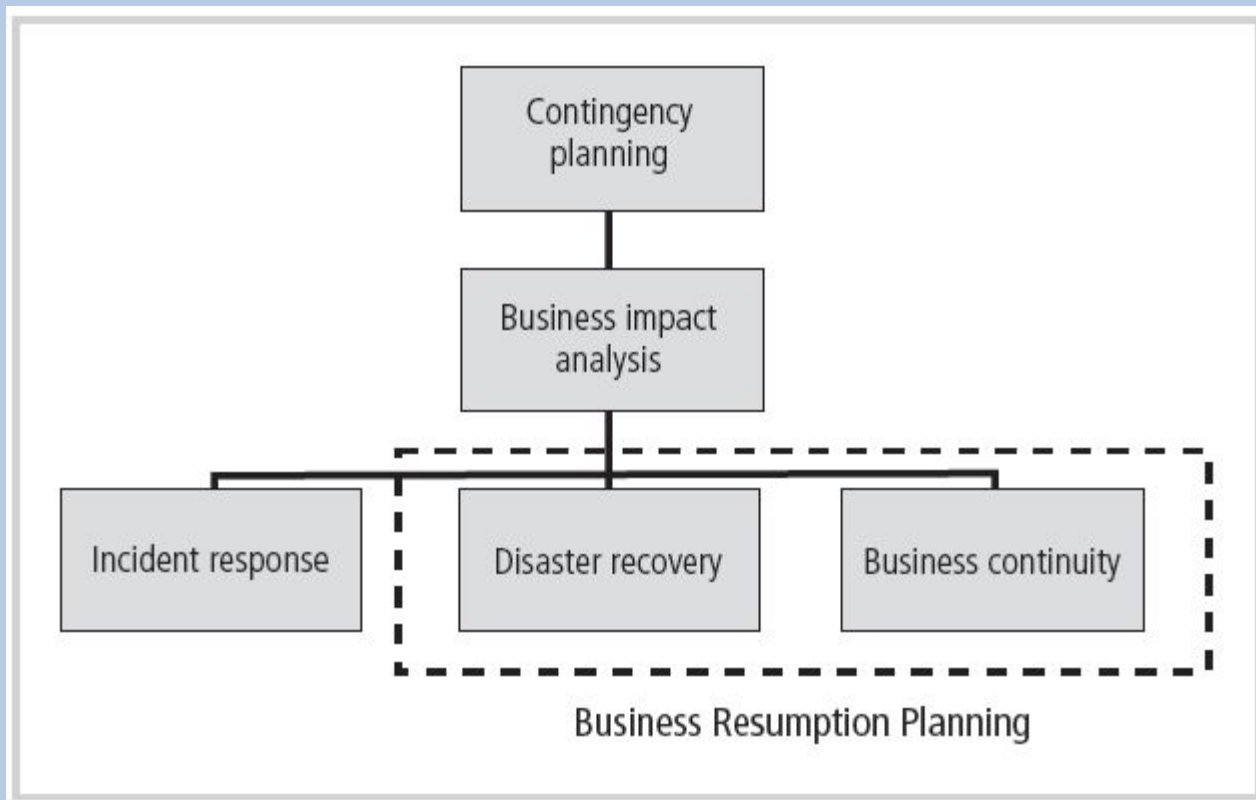


Figure 5-14 Components of Contingency Planning

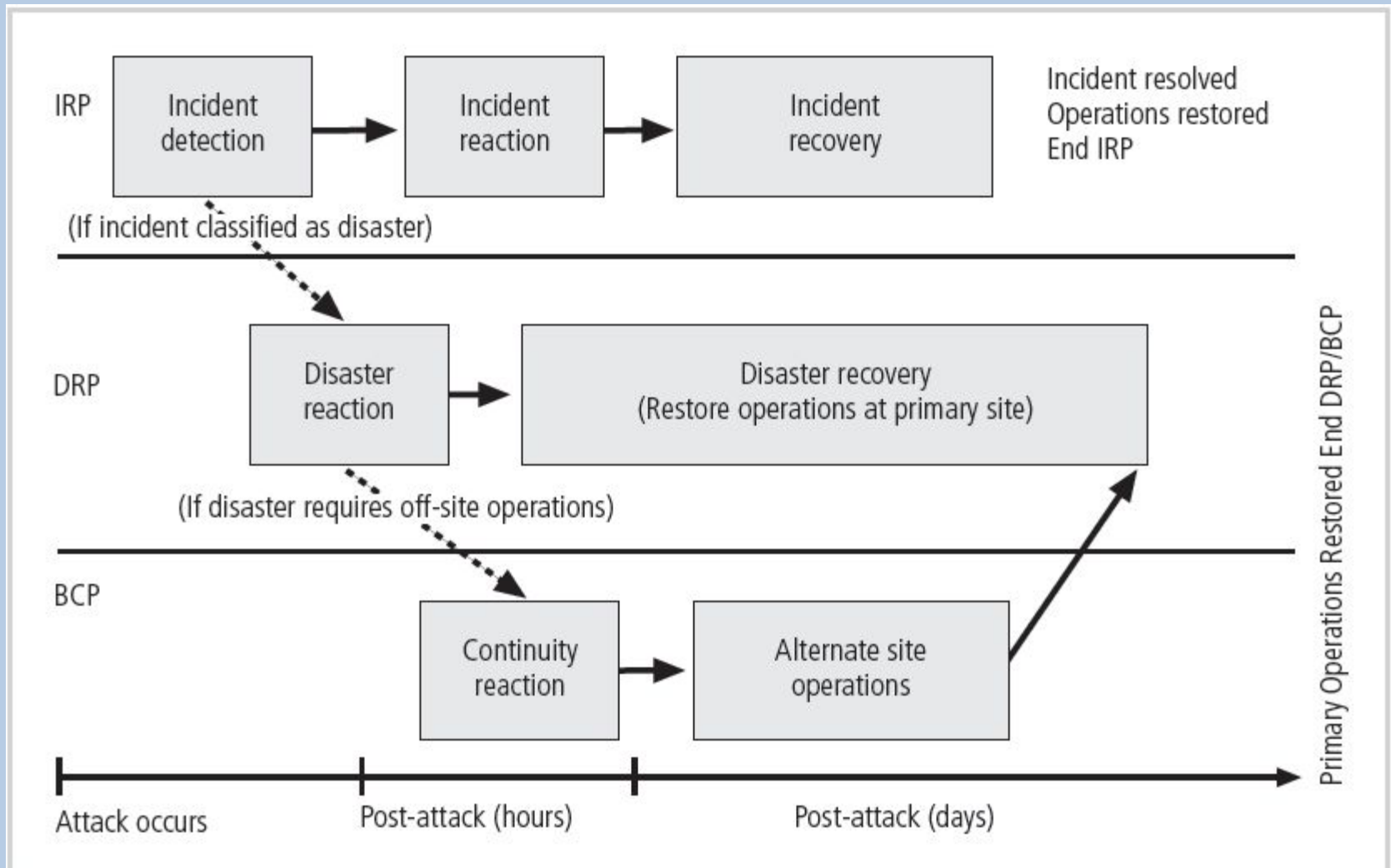


Figure 5-15 Contingency Planning Timeline

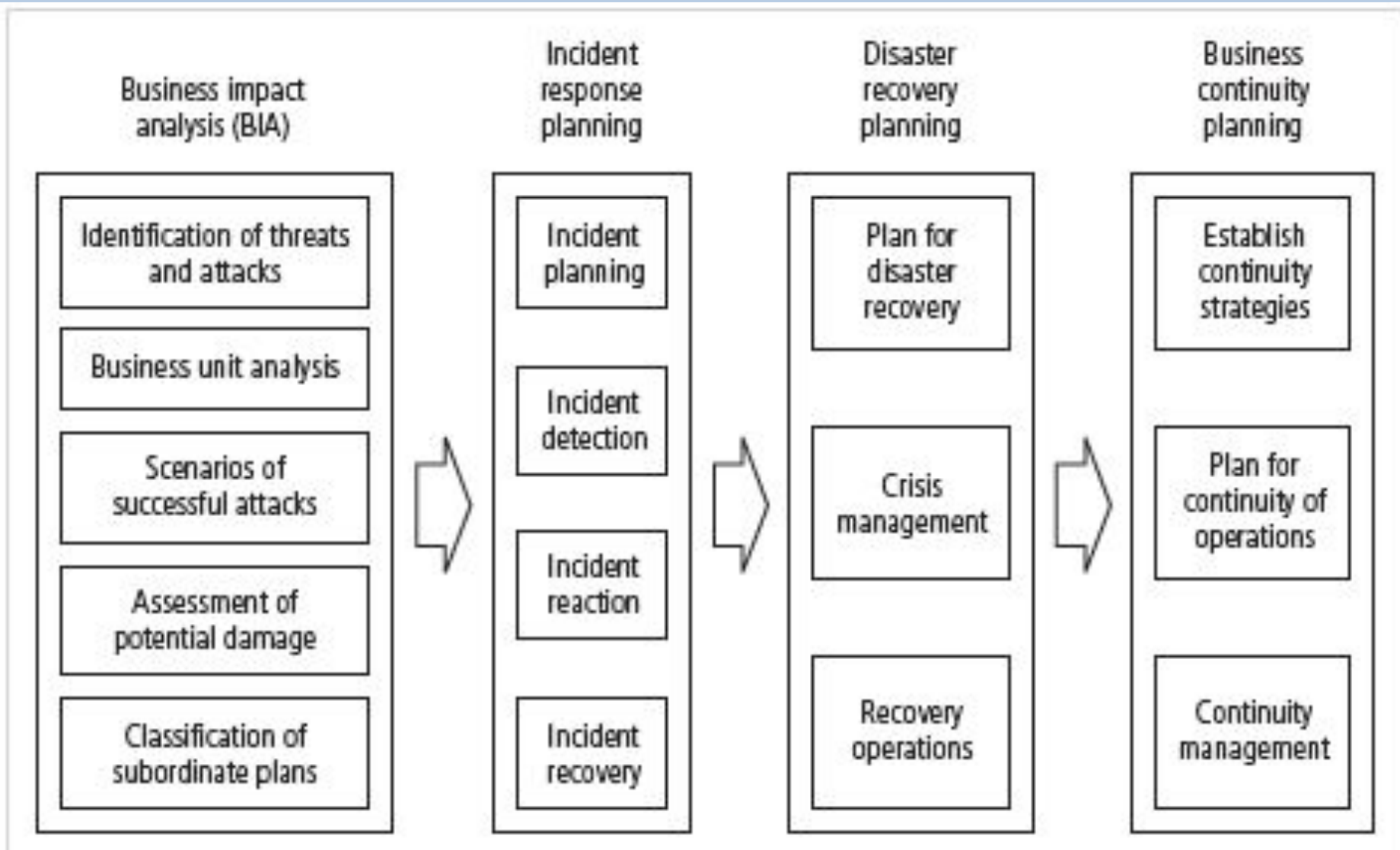


Figure 5-16 Major Steps in Contingency Planning

YOU HAVE DONE ENOUGH TODAY