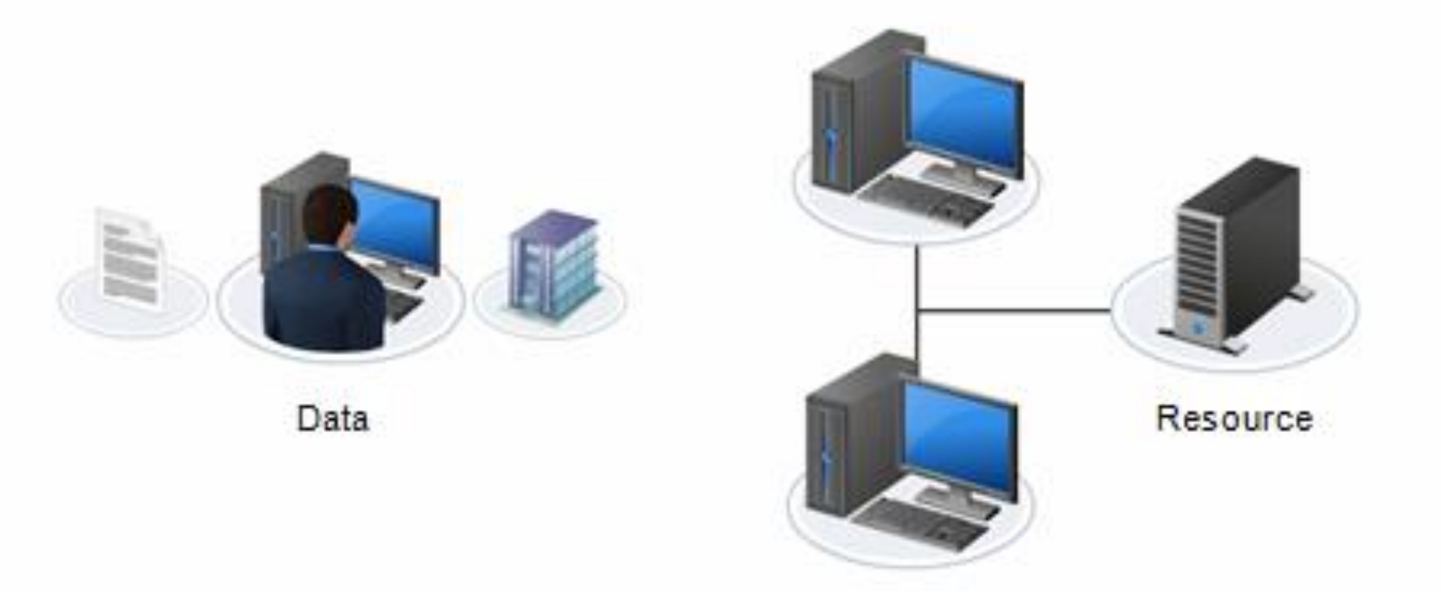
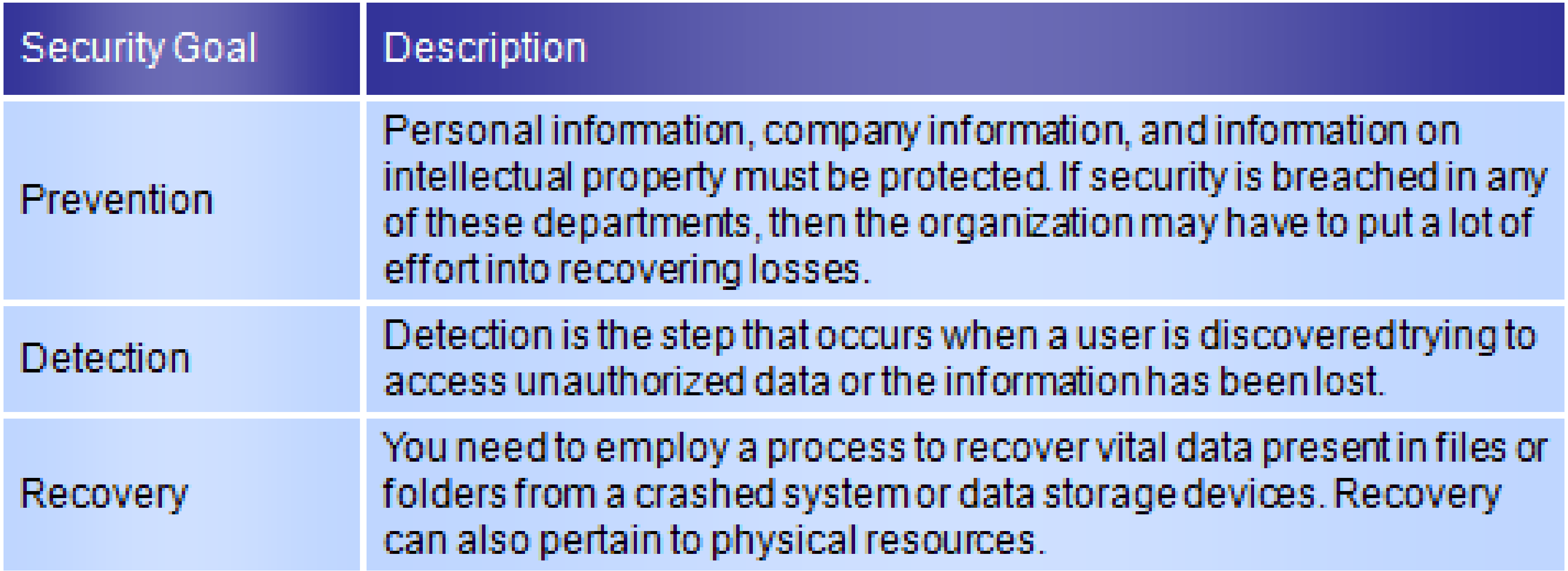
CompTIA Security+

2.0 Compliance and Operational Security

What is information security?



Goals of Security



Security Goal	Description
Prevention	Personal information, company information, and information on intellectual property must be protected. If security is breached in any of these departments, then the organization may have to put a lot of effort into recovering losses.
Detection	Detection is the step that occurs when a user is discoveredtrying to access unauthorized data or the information has been lost.
Recovery	You need to employ a process to recover vital data present in files or folders from a crashed system or data storage devices. Recovery can also pertain to physical resources.

Objective 2.1

- Explain the importance of risk related concepts

Controls

- Controls are put in place to close vulnerabilities, prevent exploitation, reduce the threat potential, and/or reduce the likelihood of a risk or its impact.

*Risk Control Types

- Technical
  - Think firewalls, IDSs/IPSs, etc…
- Management
  - Think policies
- Operational
  - Think physical security

*Exam Alert

- Controls are intended to mitigate risk in some manner, but at times they might fail in operation
  - **False Positive:** occurs when an alarm or alert is triggered by benign or normal events.
  - **False Negative:** occurs when an alarm or alert is not triggered by malicious or abnormal events.
  - Did it detect it? Positive or Negative
  - Did it get it correct? True or False

Risk Reduction Policies

- Privacy policy (PII)
- Acceptable use policy (what is allowed)
- Security policy
- Mandatory vacations procedures
- Job rotation procedures (cross training)
- Separation of duties
- Least privilege guidelines

Privacy Policy

- Private sensitive information is referred to as personally identifiable information (PII)
- This is any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains

Acceptable Use Policy (AUP)

- An organization's acceptable use policy must provide details that specify what users may do with their network access

- This includes email and instant messaging usage for personal purposes, limitations on access times, and the storage space available to each user

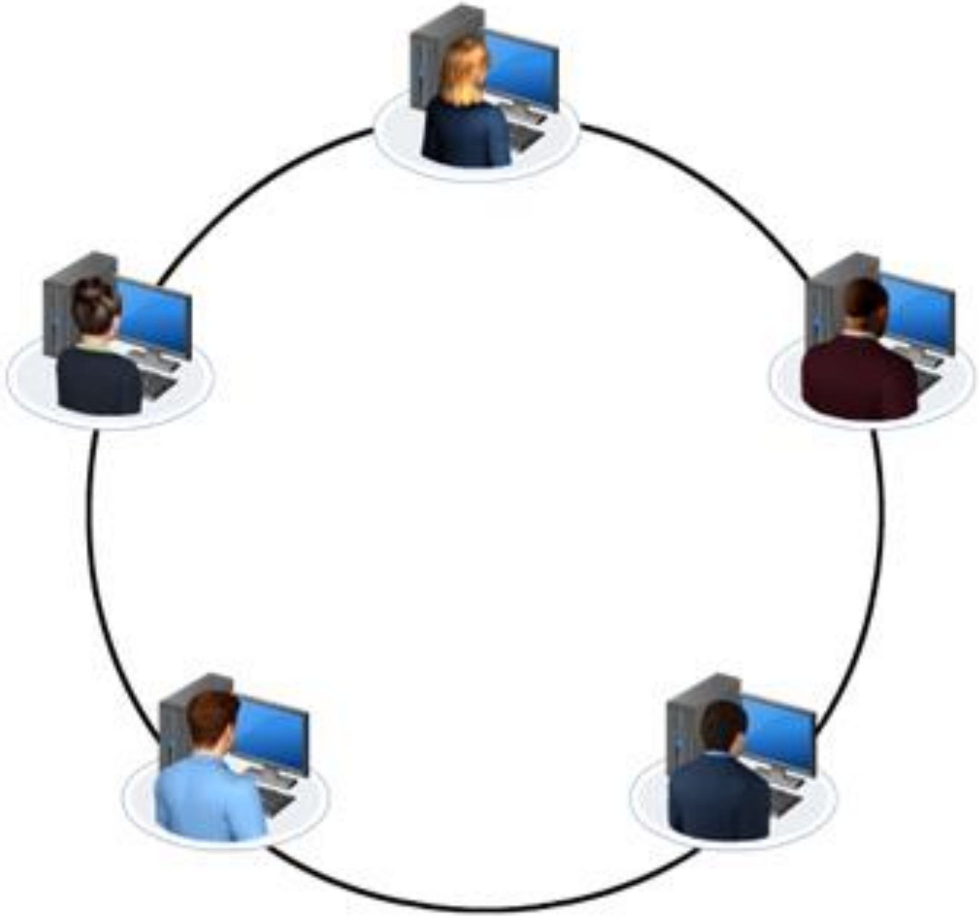
- It is important to provide users the least possible access rights while allowing them to fulfill legitimate actions

Security Policy

- An organization should have a clear outline that is created by senior management that addresses all areas of security
- This includes acceptable use, physical security, privacy, job roles and responsibilities, and least privilege guidelines
- It is important for all personnel to have access to the security policy as a means of keeping them informed and to allow for all personnel to adjust to changes that support this policy.
- Everyone is responsible for security

Mandatory Vacations

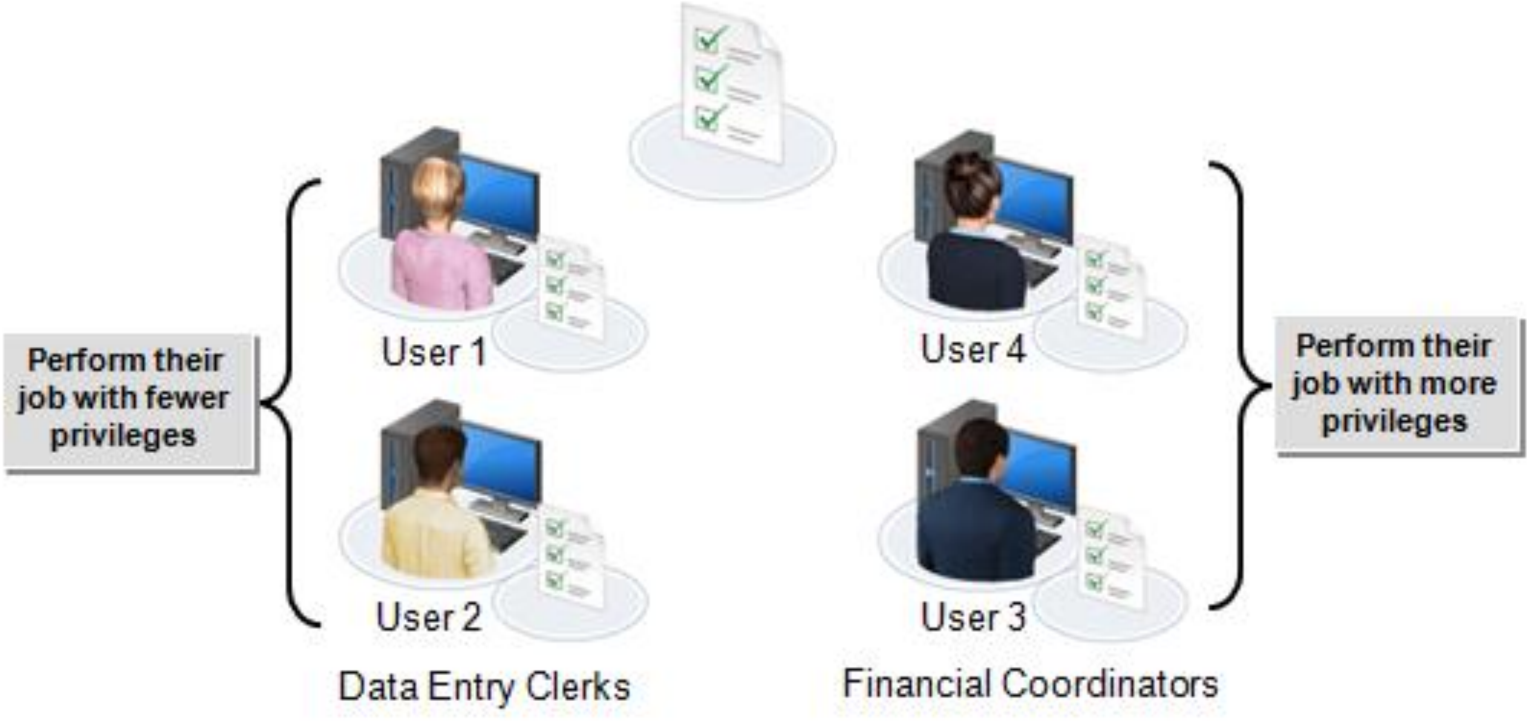
Job Rotation



Separation of Duties

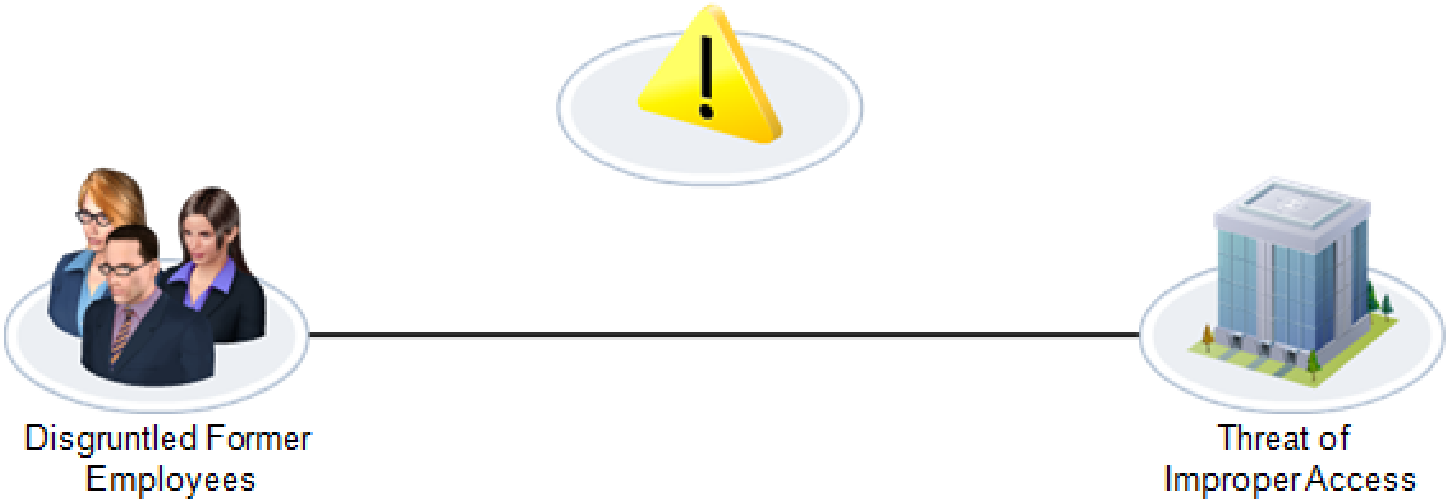
Audit
Backup
Restore

Least Privilege


Perform their job with fewer privileges
User 1
User 2
Data Entry Clerks
User 4
User 3
Financial Coordinators
Perform their job with more privileges

Risk

- Risk is the likelihood that a threat can exploit a vulnerability to cause some type of damage



*Risk Calculation

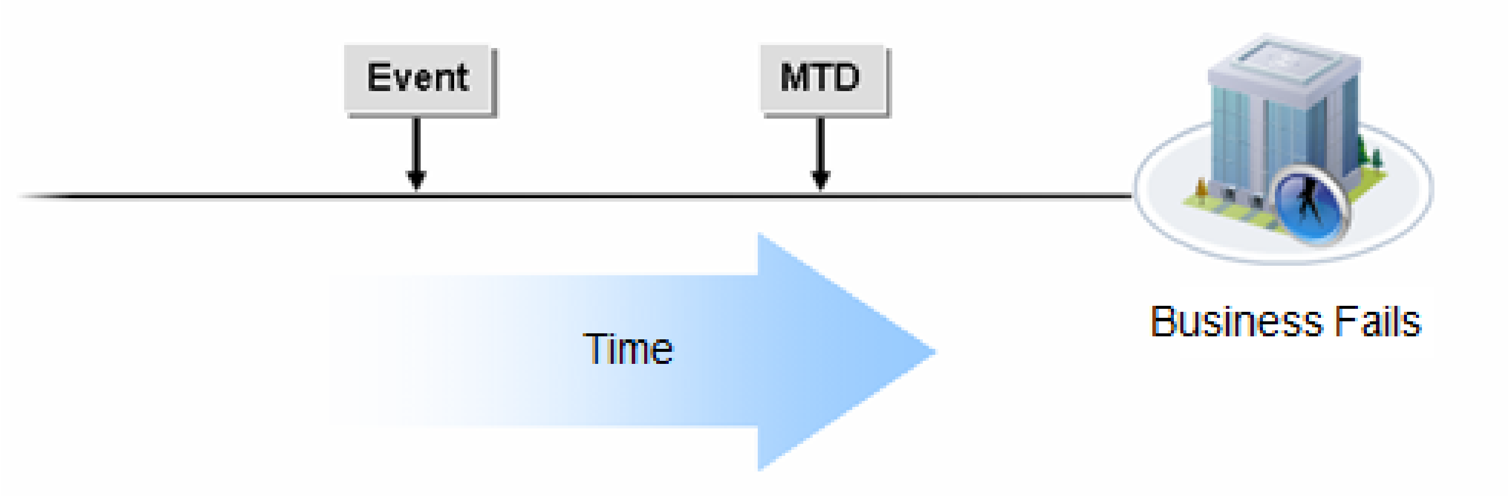
- Likelihood
  - How often do you expect it to occur?
  - Annual Rate of Occurrence (ARO)

- Single Loss Expectancy (SLE)
  - What is the monetary loss if a single event occurs?
  - Asset Value (AV) x Exposure Factor (EF)

- Annual Loss Expectancy (ALE)
  - ARO x SLE

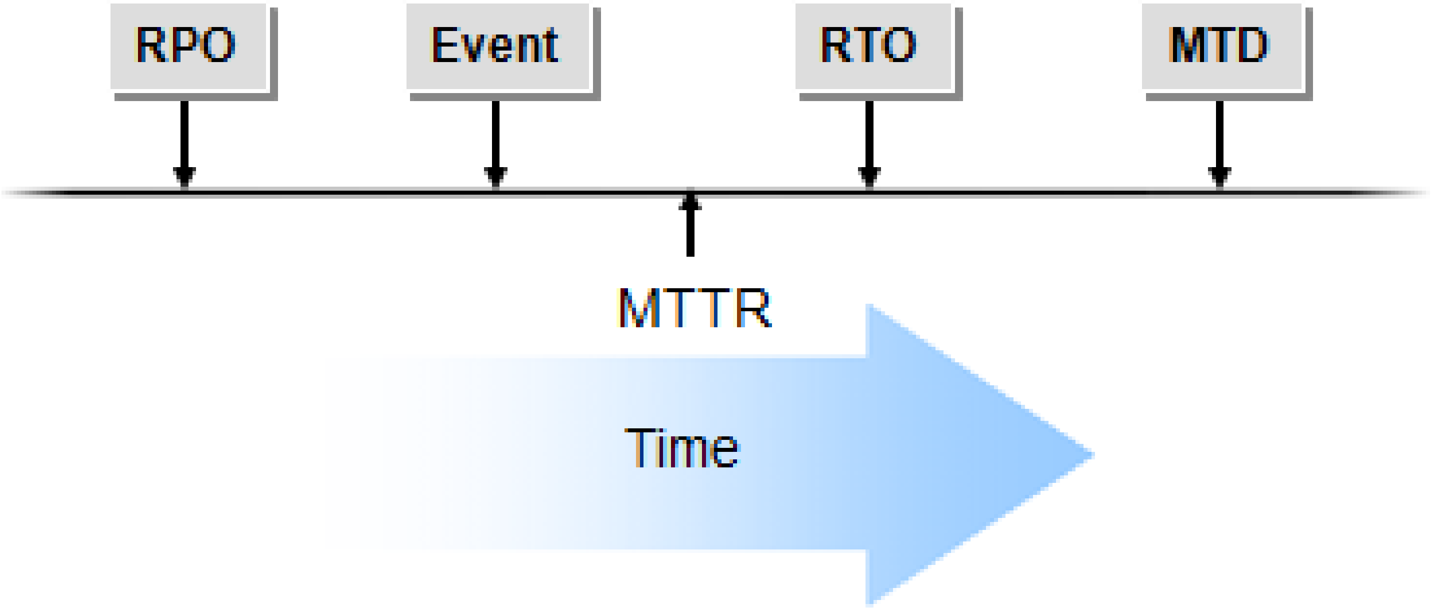
Maximum Tolerable Downtime (MTD)

The maximum length of time a business function can be discontinued without causing irreparable harm to the business.



Mean Time To Restore (MTTR)

Average time that it will take to recover from any failure



Mean Time Between Failures (MTBF)

- The rating on a device or devices that predicts the expected time between failures

- High Availability
  - Rating that expresses how closely systems approach the goal of providing data availability 100% of the time
  - Five nines = 99.999% = 5.3 minutes a year

- Service Level Agreements (SLA)
  - Between you and a provider

- MTTF: Mean Time To Failure
  - Very similar to MTBF

Qualitative vs Quantitative

- **Quantitative** allows for the clearest measure of relative risk and expected return on investment or risk reduction on investment.

- **Quantitative** is (numerical)

- **Qualitative** uses processes to determine asset worth and valuation to the organization.

- **Qualitative** is (subjective/relative)

Vulnerability

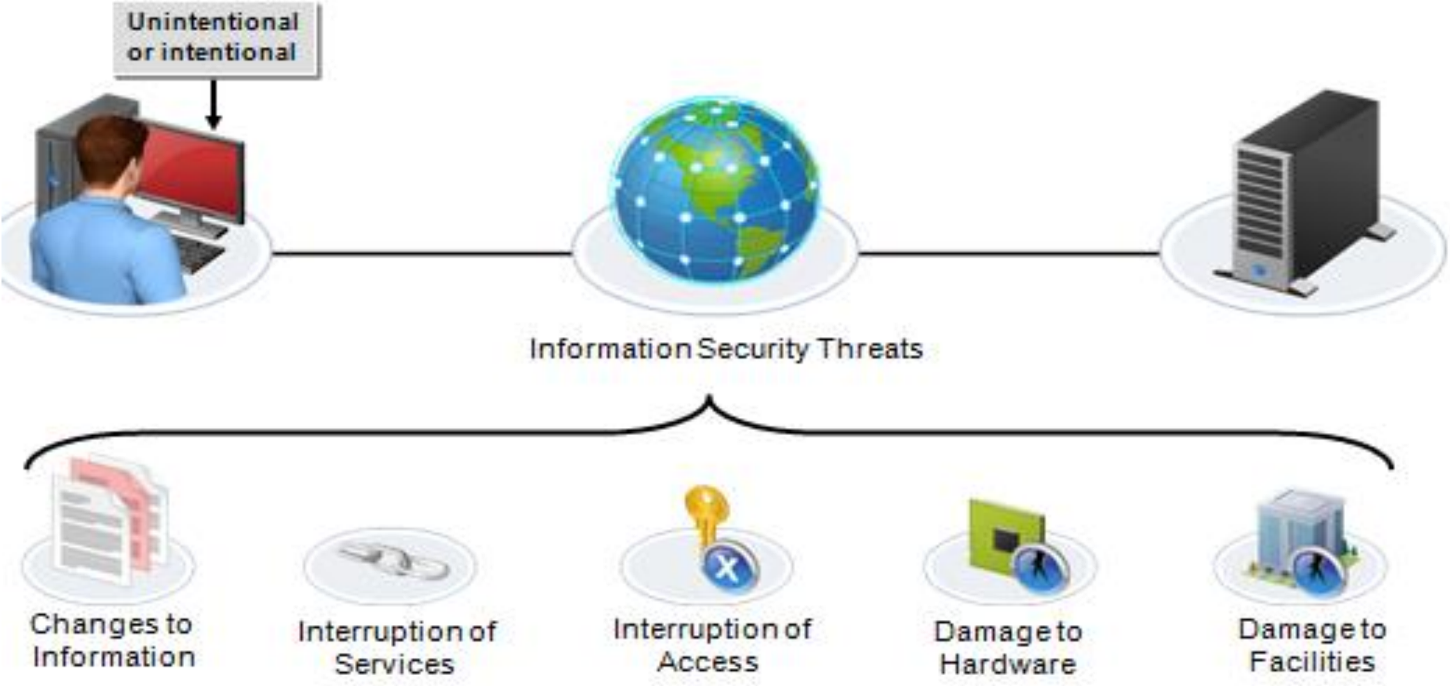
- An opening or weakness

Threat Vectors

- A ***Threat Vector*** is a path or a tool that a ***Threat Actor*** uses to attack the target

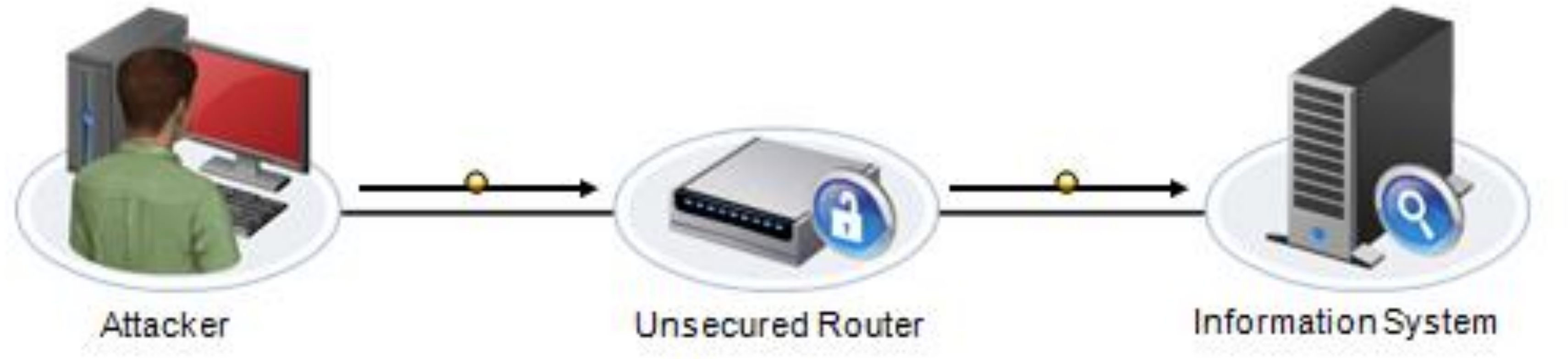
Threat

- An event or action that could potentially result in a security violation



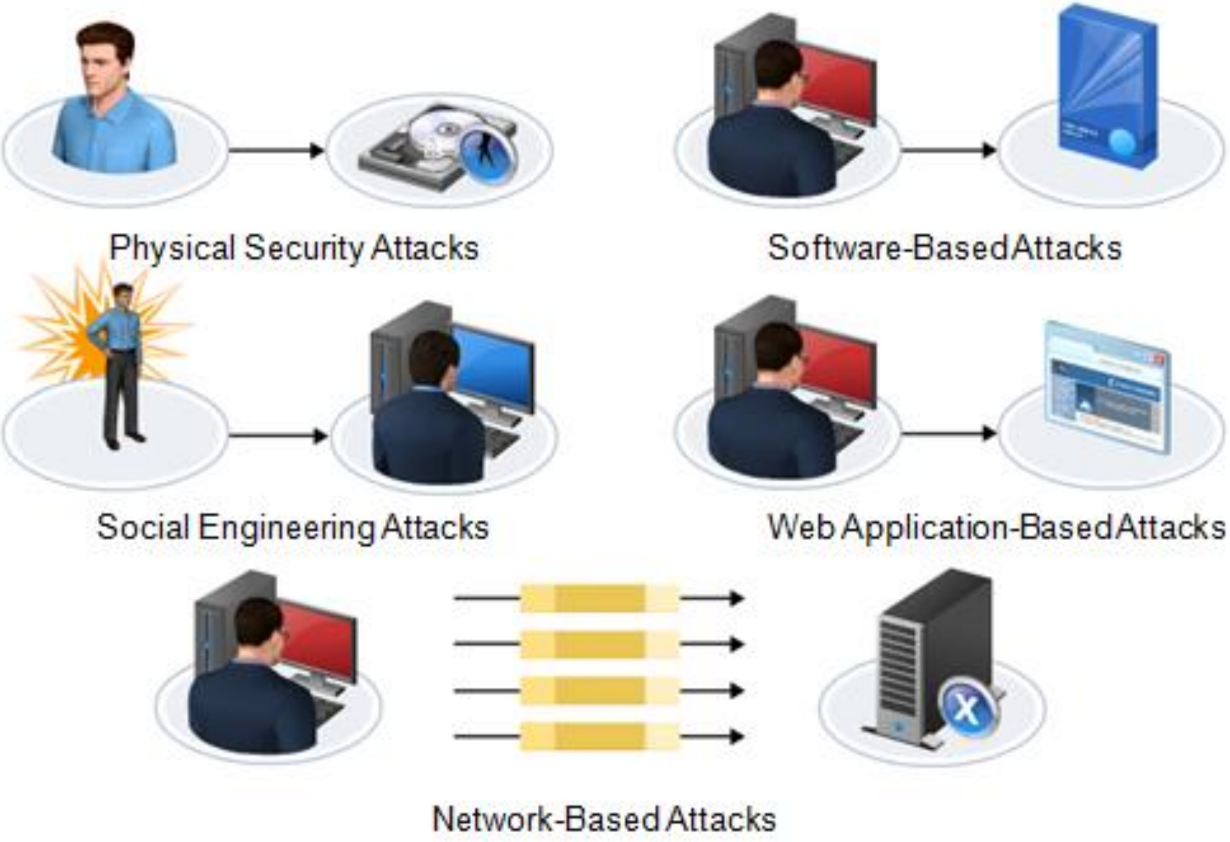
Exploit

- A mechanism of taking advantage of an identified vulnerability



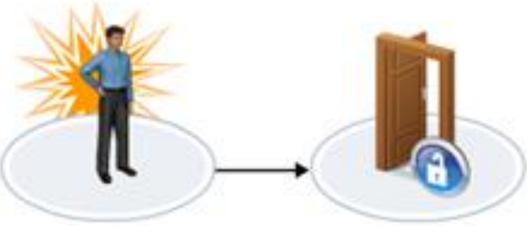
Attack

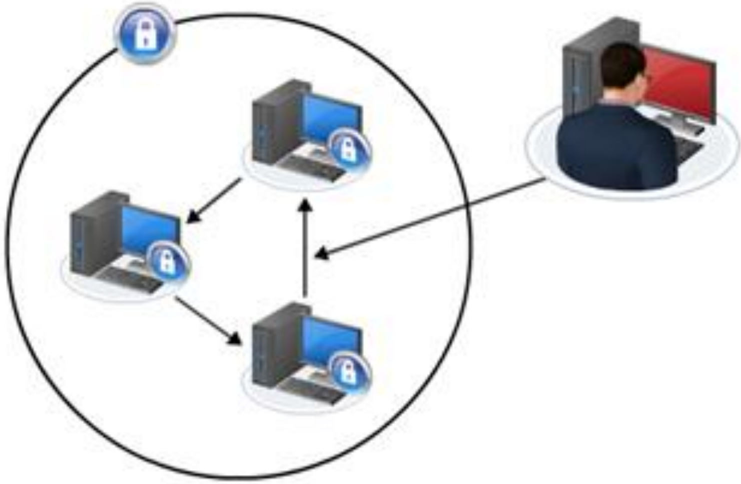
- A technique used to exploit a vulnerability


Physical Security Attacks
Software-Based Attacks
Social Engineering Attacks
Web Application-Based Attacks
Network-Based Attacks

Intrusion

- Occurs when attacker accesses your system without authorization





Risk Responses

- Risk management deals with the alignment of five potential responses with an identified risk:
- **1. Acceptance:** Often the choice made when implementing any of the other four choices exceeds the value of the harm that would occur if the risk came to fruition
- **2. Avoidance:** Involves identifying the risk and making the decision to no longer engage in the actions associated with that risk

Risk Responses

- **3. Mitigation:** When steps are taken to reduce the risk

- **4. Deterrence:** Involves understanding something about the enemy and letting them know the harm that can come their way if they cause harm to you

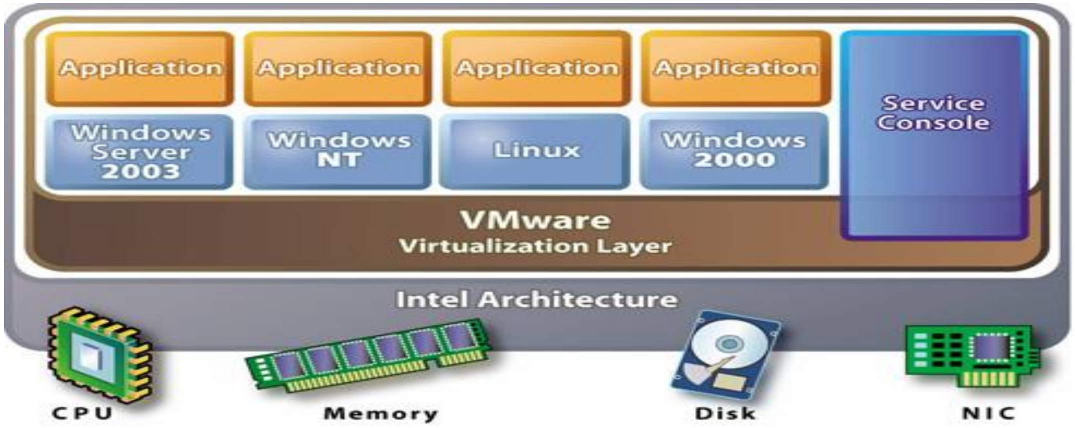
- **5. Transference:** Share some of the burden of the risk with someone else, such as an insurance company

Risks associated with Cloud Computing

- Control of data
- Security is managed by 3rd party
- Server availability
- Account lockout

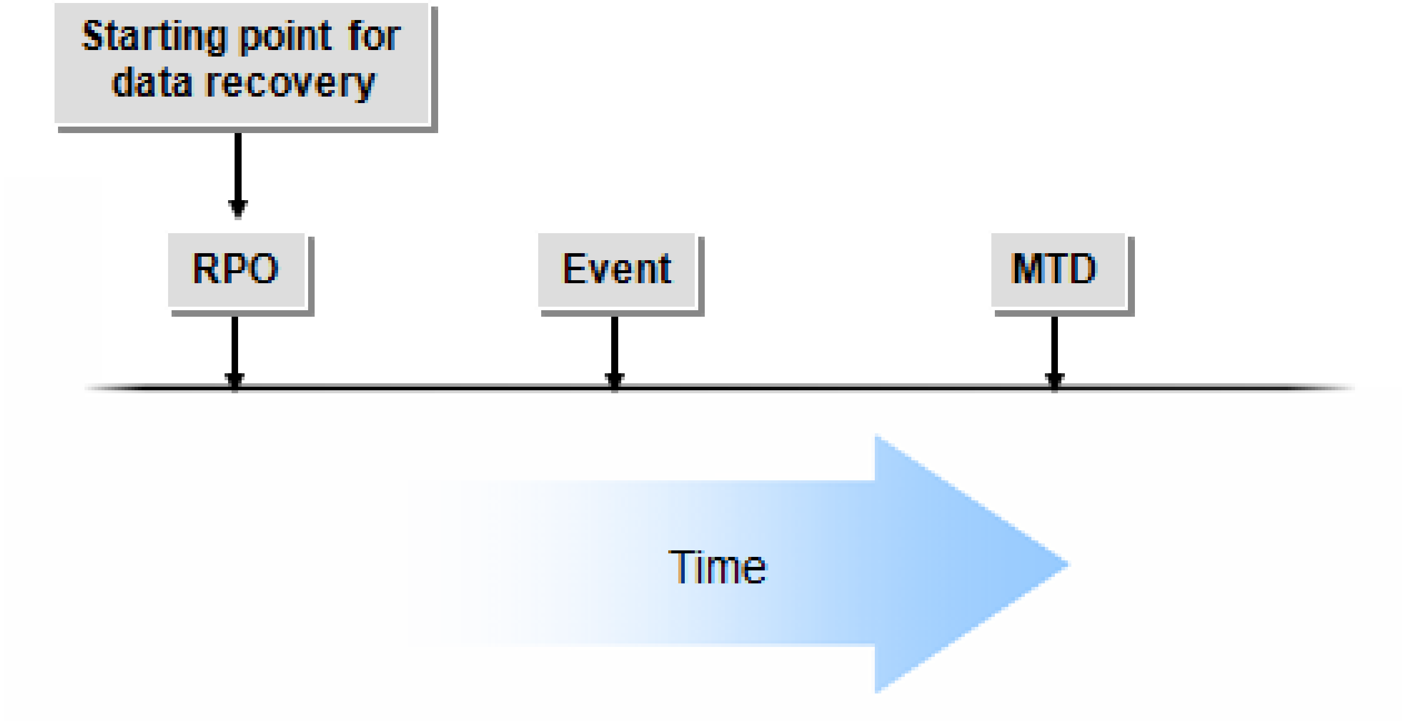
Risks associated with Virtualization

- Don’t do patches and updates on all VMs
- Compromising virtualization layer puts all systems at risk
- Little control over VM to VM communication
  - Not much support for “virtualized firewalls”
- Virtualization server contains VMs that have different security profiles
- Potential loss of Separation of Duties



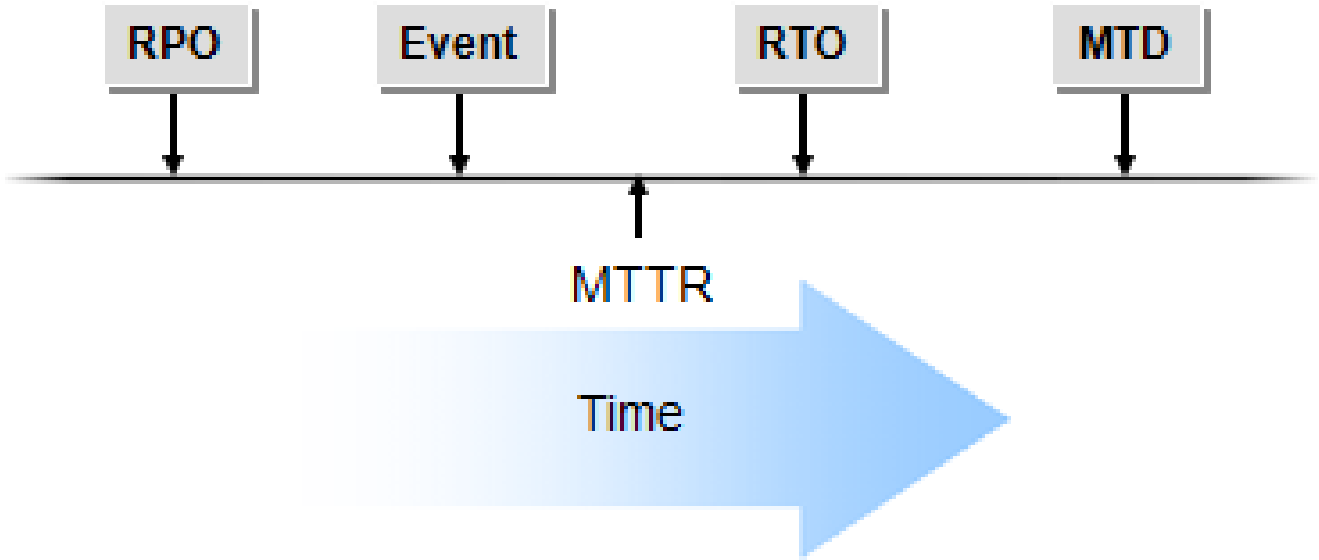
Recovery Point Objectives (RPO)

The age of files that must be recovered from backup storage for normal operations to resume



Recovery Time Objectives

Amount of time the business can be without the service, without incurring significant risks or significant losses



Student Check

When a user signs a(n) __________, it’s a form of consent to the monitoring and auditing processes used by the organization.

○ A. Acceptable use policy
○ B. Privacy policy
○ C. Separation of duties policy
○ D. Code of ethics policy

Student Check

When a user signs a(n) __________, it’s a form of consent to the monitoring and auditing processes used by the organization.

- ○ A. Acceptable use policy
- ○ B. Privacy policy
- ○ C. Separation of duties policy
- ○ D. Code of ethics policy

*Student Check

Which of the following risk-assessment formulas represents the total potential loss a company may experience within a single year due to a specific risk to an asset?

○ A. EF
○ B. SLE
○ C. ARO
○ D. ALE

Student Check

Which of the following risk-assessment formulas represents the total potential loss a company may experience within a single year due to a specific risk to an asset?

○ A. EF

○ B. SLE

○ C. ARO

○ D. ALE

Student Check

A risk has the following calculated values Single Loss Expectancy (SLE) = $1,500, Annual Rate of Occurrence (ARO) = 5. What is the maximum amount that should be spent to fully mitigate the costs of this risk?

❍ **A. $300**
❍ **B. $500**
❍ **C. $1,500**
❍ **D. $7,500**

Student Check

A risk has the following calculated values Single Loss Expectancy (SLE) = $1,500, Annual Rate of Occurrence (ARO) = 5. What is the maximum amount that should be spent to fully mitigate the costs of this risk?

- ○ A. $300
- ○ B. $500
- ○ C. $1,500
- ○ D. $7,500

Student Check

Regarding qualitative versus quantitative measures, which of the following statements is true?

○ A. Quantitative measures evaluate risk based on a subjective assessment

○ B. Qualitative measures are less precise

○ C. Qualitative measures are easier to measure for ROI/RROI

○ D. Quantitative measures are always better than qualitative measures

Student Check

Regarding qualitative versus quantitative measures, which of the following statements is true?

○ A. Quantitative measures evaluate risk based on a subjective assessment

○ B. Qualitative measures are less precise

○ C. Qualitative measures are easier to measure for ROI/RROI

○ D. Quantitative measures are always better than qualitative measures

Student Check

Which policy details what users may do with their network access?

○ A. Privacy
○ B. Acceptable Use
○ C. Storage and Retention
○ D. Secure Disposal

Student Check

Which policy details what users may do with their network access?

- ○ A. Privacy
- ○ B. Acceptable Use
- ○ C. Storage and Retention
- ○ D. Secure Disposal

Student Check

The policy preventing too much power leading to corruption is called the ____________________ policy.

○ A. Account Provisioning
○ B. Least Privilege
○ C. Separation of Duties
○ D. Acceptable Use

Student Check

The policy preventing too much power leading to corruption is called the ___________________ policy.

○ A. Account Provisioning
○ B. Least Privilege
○ C. Separation of Duties
○ D. Acceptable Use

Objective 2.2

Security Implications of integrating systems and data with third parties

On-boarding/ Off-boarding partners

- On-Boarding is the process of adding new employees to the identity and access management (IAM) system of an organization

- Off-Boarding is the reverse of this process in that it is the removal of an employee’s identity from the IAM system once they have left the organization

- Changes to a roll or privilege state can be cause for use of either of these processes

Social media networks and/or applications

- Networks such as Facebook, Twitter, LinkedIn and other applications such as Instagram, WeChat and Vine

- Organizations do not have full control over the message received by the public

- Great risk of exposure or negative reflection upon your organization is involved with Social Media

Interoperability Agreements

- SLA: Service Level Agreement
- BPA: Business Partners Agreement
- MOU: Memorandum of Understanding
- ISA: Interconnection Security Agreement

Service Level Agreement (SLA)

- Contracts with ISPs, utilities, facilities managers, and other types of suppliers that detail minimum levels of support that must be provided (including in the event of failure or disaster).

- Uptime is based on 365 days/year, 24 hours/day

99.9999%	31.5 seconds downtime/year
99.999%	5.3 minutes downtime/year
99.99%	53 minutes downtime/year
99.9%	8.76 hours downtime/year
99%	87.6 hours downtime/year

BPA

- Business Partners Agreement
- A contract between two entities dictating their business relationship
- Clearly defines the expectations of each partner
- Includes details about the many processes of the business agreement

MOU

- Memorandum of Understanding
- A formal agreement between two entities
- Can also be called a letter of intent
- It specifies an agreement between two parties without legal bind to the document
- Essentially a handshake on paper

ISA

- Interconnection Security Agreement

- Formal declaration of the security stance, risks, and technical requirements of a link between two organizations IT infrastructures

- This defines the expectations and responsibilities of maintaining security over a communications path between two networks

Privacy considerations

- Privacy considerations in relation to integrated systems and data with third parties should be taken seriously

- Should be outlined in the organization Privacy Policy

Risk awareness

- Involves evaluating assets, vulnerabilities, and threats in order to clearly define an organization's risk level

Unauthorized data sharing

- Can lead to the disclosure of private, confidential or proprietary data
- There is an increased risk of unauthorized data sharing when working with third parties
- Ex: Target security violation
- Encryption, authentication, authorization control and monitoring of activities can reduce the risk

Data ownership

- It is important to clearly establish rules and restrictions regarding data ownership

- Third party involvement requires this

- Does the original possessor of the data retain ownership?
- Does anyone receiving the data now have ownership?
- Or does the intermediary supporting network or communications path have potential ownership of transferred data?

Data backups

- Essential to data recovery in the event of loss or corruption

- Third party involvement in a data system can result in an issue determining what is to be backed up and whom is responsible

- Data ownership needs to be addressed when dealing with backups

Follow security policy and procedures

- Ensure that when integrating systems with third parties that there are no significant gaps between the levels of security between the organizations

Review agreement requirements to verify compliance and performance standards

- Both sides, internal and external, should audit their partner for compliance with the mutual agreements as well as compliance with any regulation or contractual obligation
- In the event of a violation, both parties may be held responsible for the oversight
- Both parties can benefit from access to each other's security acumen for auditing purposes

Exam Alert

- Understand security implications of integrating systems and data with third parties
- Whenever a third party is involved in your IT infrastructure, there is an increased risk of data loss, leakage, or compromise

Student Check

Which of the following is more formal than a handshake agreement but not a legal binding contract?

- A. SLA
- B. BIA
- C. DLP
- D. MOU

Student Check

Which of the following is more formal than a handshake agreement but not a legal binding contract?

- ○ A. SLA
- ○ B. BIA
- ○ C. DLP
- ○ D. MOU

Objective 2.3

- Implement appropriate risk mitigation strategies

Change Management

Good change management practices can mitigate unintentional internal risks caused by inappropriate alterations to systems, tools, or the environment

Change management should be used to oversee alterations to every aspect of a system, including hardware configuration and OS and application software

- Have clear policies
- Testing
- Documentation

Incident Management

- Event: Any occurrence that takes place during a certain period of time

- Incident: An event that has a **negative outcome** affecting the confidentiality, integrity, or availability of an organization’s data

- Good management strategies mitigate the severity of damage caused by risks

- Technical steps and documentation for handling systems and preserving evidence
  - **Forensic procedures**

User Rights and Permissions Reviews

- Be sure to review user rights and permissions **periodically** (Annually) to make sure they meet your needs for confidentiality as well as accessibility of information and resources

Perform Routine Audits

- Perform routine audits to assess the risk of a particular operation and to verify that the current security controls in place are operating properly

- Double checking that policies are being implemented

- Might need to bring in a 3rd party

- Types
  - Privilege audits
  - Usage audits
  - Escalation auditing
  - Disaster Recovery Plan (DRP)
  - Administrative auditing
  - Documentation

Enforce policies and procedures to prevent data loss or theft

- Address concerns of data loss or theft
- Precautions, preventions, and deterrents must be implemented that reduce risk of theft
- Backup and restoration processes can help prevent data loss due to accident, oversight, malicious code or intentional attacks
- Disclosure of information due to loss or leakage (spillage) should be addressed in a Data Loss Prevention (DLP) solution (covered later)

Process of Analysis

- Identify Vulnerabilities
  - Port Scans, Vulnerability Scans
- Identify Risks
- Measure Risks
  - Cost/Benefit comparison
- Identify Assets
  - The original cost, the replacement cost, its worth to the competition. its value to the organization, maintenance costs, and the amount it generates in profit

Components of Risk Analysis

Vulnerability × Threat = Amount of risk

Risk Matrix

Risk	Annual Rate of Occurrence (ARO)	Single Loss Expectancy (SLE)	Annual Loss Expectancy (ALE)	Mitigation
Flood damage	5	$19,000	$95,000	Flood insurance
Electrical failure	2	$50,000	$100,000	Generator, UPS
Flu epidemic	4	$50,000	$200,000	Flu shots

Implement security controls based on risk

- Risk mitigation techniques can be applied at many levels of an organization to help guard against potential risk damage

Data Loss Prevention (DLP)

- Data Loss Prevention (DLP) is the idea of systems specifically implemented to detect and prevent unauthorized access

- Can include hardware and software elements designed to support this primary goal

- Do what you can to prevent loss of data, bit locker

Objective 2.4

- Implement basic forensics procedures

Computer Forensics

Major concepts behind computer forensics

- Identify the evidence
- Determine how to preserve the evidence
- Extract, process, and interpret the evidence
- Ensure that the evidence is acceptable in a court of law

Computer Forensics

- **Establish a clear chain of custody**
- Properly collect the evidence
- Correctly perform the investigation
- Document all actions and findings
- Preserve all evidence and documentation
- Prepare to provide expert testimony or consultation if required

Basic Forensic Procedures

- Order of volatility
  - Cache, Routing and ARP tables, RAM, Virtual Memory and Temporary File Systems(Swap Files), HDDs and flash drives, CD-ROMs, DVD-ROMs and printouts
- Capture system image
  - A bit-for-bit copy
  - Use a hardware write-blocker
  - Take hashes
- Network traffic logs
  - Firewall logs
  - IDS/IPS logs

Basic Forensic Procedures

- Capture video
    - A moving record of the event
    - Security cameras
- Record time offset
    - Synchronize times on logs from one device to another
- Screenshots
- Witnesses
- Track man hours and expenses
    - This can be used to determine whether the expense of the event was justified

Student Check

Evidence is inadmissible in court if which of the following is violated or mismanaged?

- ○ A. Chain of custody
- ○ B. Service-level agreement
- ○ C. Privacy policy
- ○ D. Change management

Student Check

Evidence is inadmissible in court if which of the following is violated or mismanaged?

- ○ A. Chain of custody
- ○ B. Service-level agreement
- ○ C. Privacy policy
- ○ D. Change management

Student Check

In order to preserve data against modification through the forensic review, which of the following forms of data storage should be examined first?

- ○ **A. Temporary file storage**
- ○ **B. Main memory**
- ○ **C. Secondary memory**
- ○ **D. Routing tables**

Student Check

In order to preserve data against modification through the forensic review, which of the following forms of data storage should be examined first?

- ○ **A. Temporary file storage**
- ○ **B. Main memory**
- ○ **C. Secondary memory**
- ○ **D. Routing tables**

Student Check

Which of the following steps should be performed first in a forensic investigation?

❍ A. Locate data
❍ B. Establish an order of volatility
❍ C. Collect data
❍ D. Review data

Student Check

Which of the following steps should be performed first in a forensic investigation?

○ A. Locate data
○ B. Establish an order of volatility
○ C. Collect data
○ D. Review data

Objective 2.5

Common incident response procedures

Preparation

- Necessary to ensure a successful outcome of unplanned downtime, security breaches, or disasters

- Includes defining a procedure to follow in response to incidents, hardening an environment against incidents, and improving detection methods

Incident identification

- The first step in incident response
  - Incident Identification
- Without detection, incidents would be false negatives
- Improved means of detection includes the use of IDS, IPS as well as monitoring of performance trends and abnormal activity levels

Escalation and Notification

- Establish a clear order of escalation
- Should be contained to individuals in specific positions of authority or responsibility
- May include legal, PR, IT staff, security staff, or HR

Mitigation steps

- Containment prevents the further spread of a problem to other systems

- Upon eliminating or reducing the damage, mitigation is responding to the incident in order to reduce risk, prevent reoccurrence, and start the recovery process

Lessons learned

- The next step in incident response
  - Documentation is final step
- Involves planning and procedures to improve mitigation strategies

- Often addresses problems with response and mistakes to avoid future incidents

Reporting

- After containment has been established, the incident response team will fully document the incident and make recommendations about how to improve the environment to prevent recurrence

- Reporting of an incident is used to provide a record of the incident, provide support for due care and due diligence

Recovery/Reconstitution Procedures

- Recovery is the process of removing any damaged elements from the environment and replacing them

- Can involve restoring from backup, removal of effected software/hardware, and updating components to new versions

First Responders

- Very specific details for first person on the scene
  - Detailed in the Incident Response Policy (IRP)
  - Contain the damage
- Don’t disturb the environment
- It’s important not to log off the system or shut down the computer, because these actions may damage or alter evidence
- Follow the escalation policy

Incident Isolation

- Quarantine separates an entity apart from the rest of an environment to provide protection

- Device Removal involves hardware that has been identified as a culprit or source of a system breach

Data Breach

- Occurs when nonpublic data is read, copied or destroyed during an incident

- The incident could be the data breach itself, or the data breach could be a consequence of the incident

Damage and Loss Control

- Involves methodologies in order to protect assets from damage

- A means of risk mitigation

- Containment: means to limit the scope of damage and prevent other systems or resources from being negatively affected

Objective 2.6

- Importance of security related awareness and training

Security policy training and procedures

- User education is mandatory to ensure that users are made aware of expectations options, and requirements related to secure access within an organization’s network
- Security training during employee orientation combined with annual training seminars is the best choice
- Role Based training should outline the responsibilities of each role in an organization

Personally Identifiable Information (PII)

- Part of Privacy Policy
- What will be done with PII?
- Not everyone understands the importance of PII

Information Classification

- Military/Government: Top Secret, Secret, Confidential, Sensitive, and Unclassified
- Corporate/Business: Confidential, Private, Sensitive, and Public
- Need-to-know
- High, Medium, Low, Confidential, Private, and Public

Data labeling, handling and disposal

- A **user** is any subject who accesses objects on a system to perform some action or accomplish a work task
- An **owner**, or information owner, is the person who has final corporate responsibility for classifying and labeling objects and protecting and storing data
- A **custodian** is a subject who has been assigned or delegated the day-to-day responsibility of properly storing and protecting objects

- Document and label everything

Compliance with laws, best practices, and standards

- Sarbanes-Oxley Act
  - Accounting compliance
- Heath Insurance Portability and Accountability Act (HIPAA)
- Fines and penalties for non-compliance

User Habits and Expectations

- Password Behaviors
- Data Handling
- Clean Desk Policies
- Prevent Tailgating
- Personally Owned Devices

Threat awareness

- New Viruses
- Phishing Attacks
- Zero Day Exploits
  - Exploiting flaws or vulnerabilities in targeted systems that are unknown or undisclosed to the world in general
- Use of social networking and P2P

Compliancy and Security Posture

- An important part of the long-term success of a security endeavor is to follow up and gather training metrics to validate compliance and security posture.

- Never assume that employees understand every aspect of their jobs or how to perform their work tasks within the boundaries of security

- Monitoring work activity, providing refresher training, and performing audits helps to assess the security compliance of personnel and improves the security posture as a whole

Follow up Training

- Because security constantly evolves with time, periodic training to add changes and to provide training for new personnel is a best practice

- New areas of importance may arise, providing reason to propose training more frequently

- Statistical analysis is very useful in building a compliance matrix, showing the effectiveness of awareness training

Student Check

Which of the following is not going to be part of a standard password policy?

○ **A. Establishing a minimum password length**
○ **B. Selection of a strong password**
○ **C. Establishing password expiration schedules**
○ **D. Barring keeping written passwords**

Student Check

Which of the following is not going to be part of a standard password policy?

○ A. Establishing a minimum password length
○ B. Selection of a strong password
○ C. Establishing password expiration schedules
○ D. Barring keeping written passwords

Student Check

When conducting data handling training and reviewing disposal practices, what consideration must be primary?

○ A. Breaches of health and safety protocols
○ B. Remnants of data that may remain accessible
○ C. Accidental disposal of equipment that is necessary to read archived legacy data
○ D. Disposal costs and penalties arising from regulatory mandates

Student Check

When conducting data handling training and reviewing disposal practices, what consideration must be primary?

○ A. Breaches of health and safety protocols
○ B. Remnants of data that may remain accessible
○ C. Accidental disposal of equipment that is necessary to read archived legacy data
○ D. Disposal costs and penalties arising from regulatory mandates

Objective 2.7

- Physical security and Environmental controls

The Importance of Environmental Controls

- Not all incidents arise from attacks, illegal activities, or other forms of directed threats to an enterprise

- Many threats emerge due to physical and environmental factors that require additional consideration in planning for security controls

HVAC

- Humidity and temperature control
  - Most experts recommend 72-76 degrees F
  - Relative humidity between 40% and 60%
- Overcooling causes condensation on equipment
- Dry environments lead to excessive static
- Positive air pressure to force contaminants out
- Monitor both locally and remotely

Fire Suppression

- The first step in a fire-safety program is fire prevention
- FM-200 replaced Halon in Datacenters
- Train employees to recognize dangerous situations and report these situations immediately
- Knowing where a fire extinguisher is and how to use it can stop a small fire from becoming a major catastrophe

EMI Shielding

- TEMPEST
  - Describes standards used to limit or block electromagnetic emanation (radiation) from electronic equipment
  - Individual pieces of equipment are protected through extra shielding that helps prevent electrical signals from emanating
- Faraday cage
  - Surrounds an object with interconnected and well-grounded metal
  - The metal used is typically a copper mesh that is attached to the walls and covered with plaster or drywall
  - The wire mesh acts as a net for stray electric signals, either inside or outside the box
- Shielded Twisted Pair (STP) and fiber cabling

Hot-Aisle/Cold-Aisle Separation

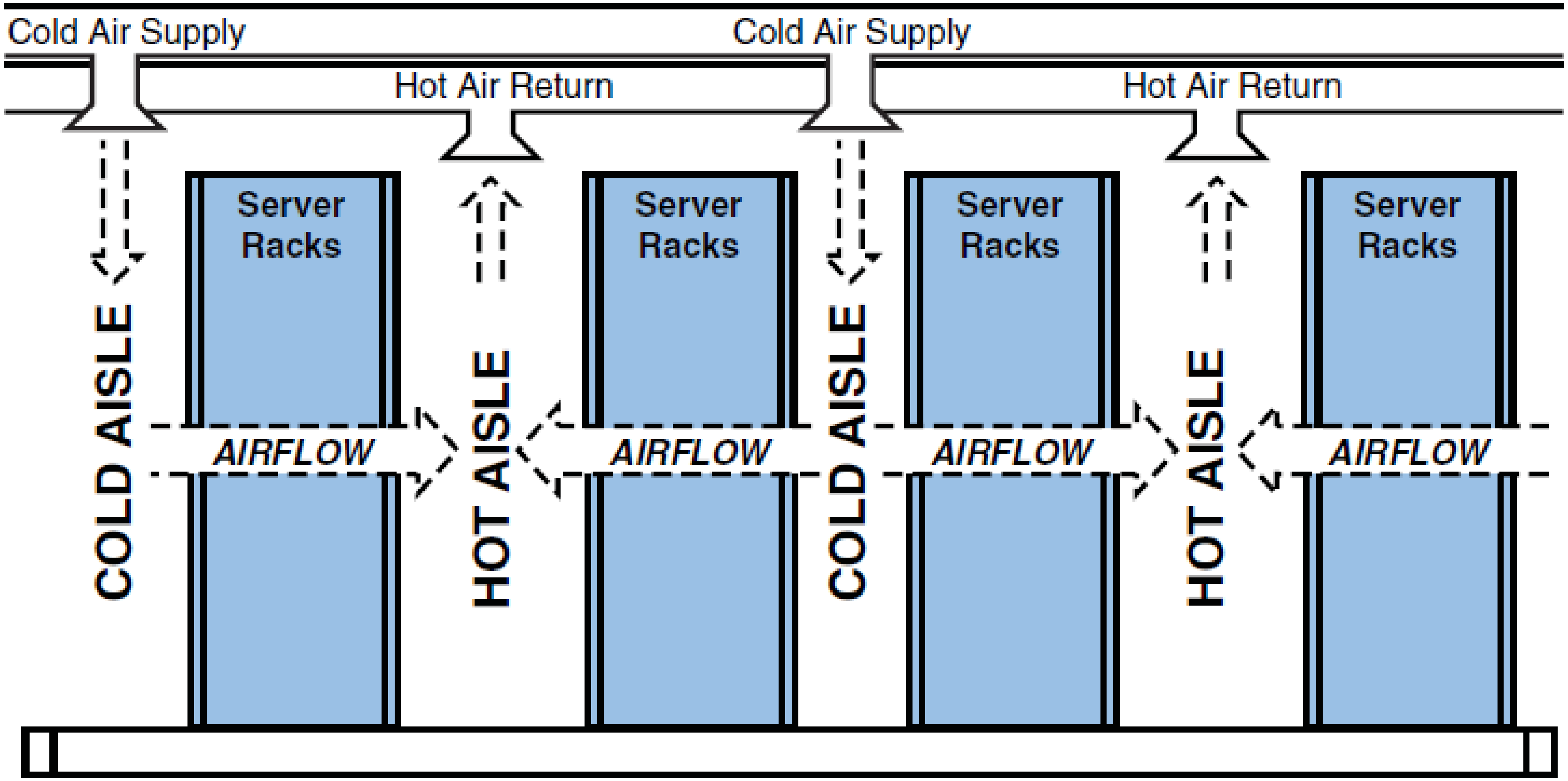


FIGURE 4.2 Simplified hot-aisle/cold-aisle data center layout with overhead HVAC supply and exhaust ducts.

Environmental Monitoring

- Best practice is to monitor all equipment/facilities according to a strict schedule both remotely, through network solutions, as well as on-site to verify accuracy

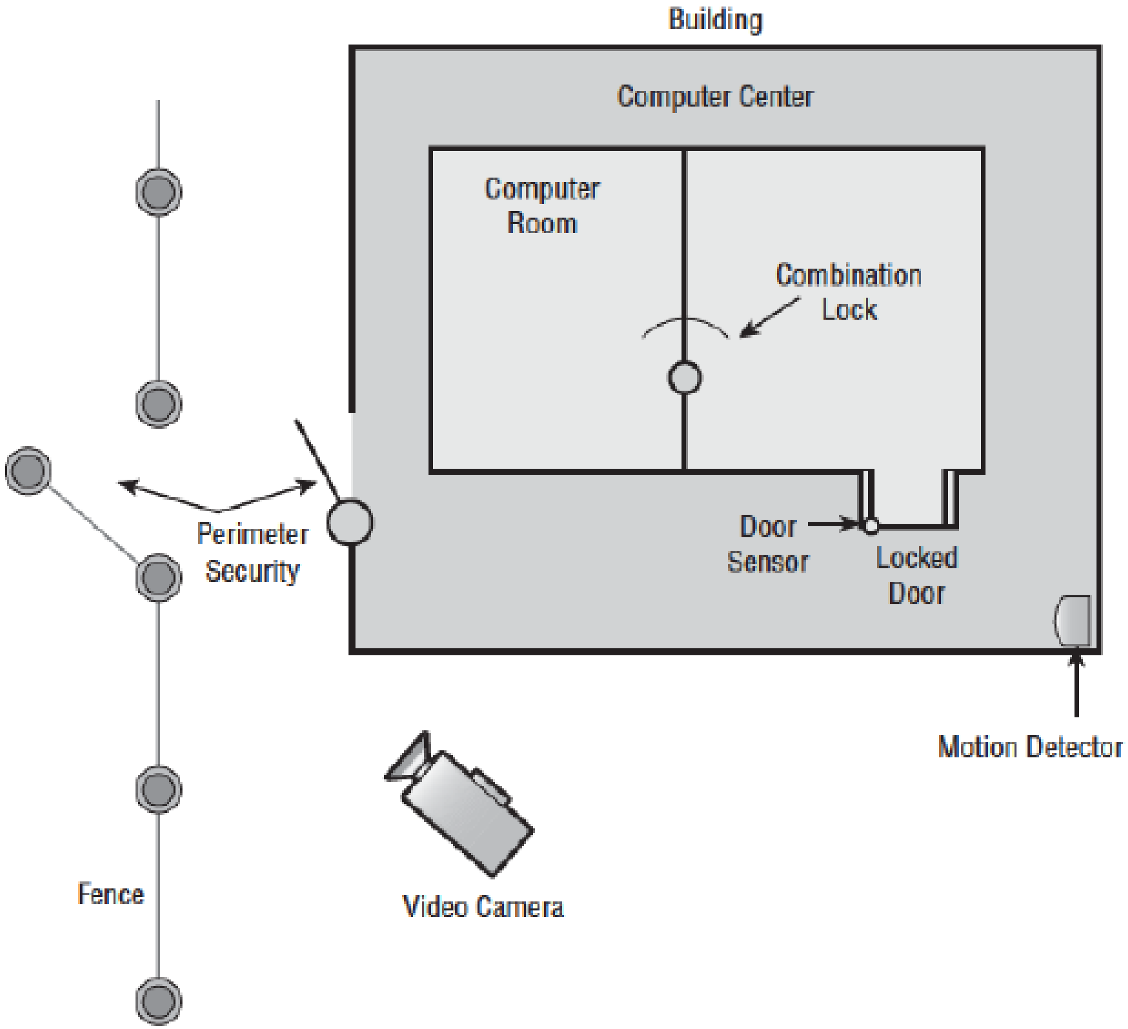
Temperature and Humidity Controls

- Temperature and Humidity management can be addressed as part of overall HVAC management or environmental monitoring

Physical Security

- To ensure proper physical security, you should design the layout of your physical environment with security in mind
- Mission-critical servers and devices should be placed in dedicated equipment rooms that are secured from all possible entrance and intrusion
- Equipment rooms should be locked at all time
- Monitoring and access logs are essential

Physical Security



Hardware locks

- Hardware locks, conventional locks, electronic or smart locks are used to keep specific doors closed and prevent unauthorized entry

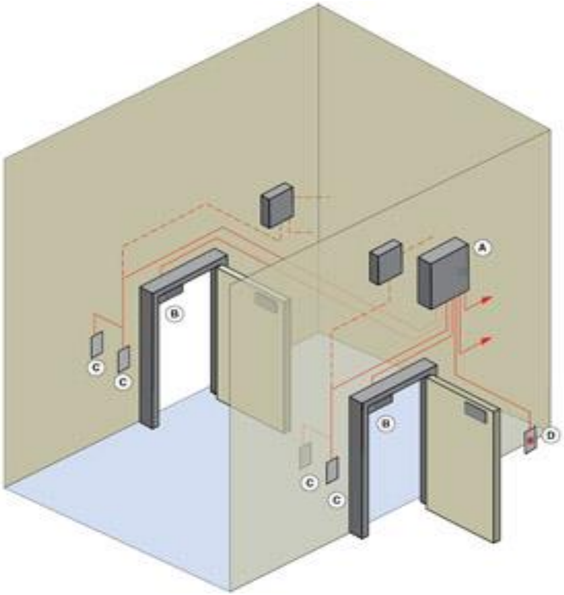
Hardware Lock

- Conventional, Deadbolt
  - Lock and key
- Electronic
  - Keyless

- Token-based
  - Magnetic swipe card or proximity reader
- Biometrics
  - Eyeballs, fingers, etc…
- Multi-factor
  - Smart card and a PIN

Mantraps

- Protects against tailgating/piggybacking
- Holding area between two entry points that gives security personnel time to view a person before allowing access



Fencing

- First line of defense in physical security
- Must review local laws and codes to ensure compliance
- Fences 3-4’ deter trespassers
- Fences 6-7’ are too hard to climb easily and deter most intruders
- Fences 8+’ with 3 strands of barbed wire deter even determined intruders
- Entry points should be strategically located for both control and safety
- Provide a means of defining the perimeter of a site

Proximity Readers

- Also called “Prox Box”
- Can be passive, field-powered or transponder driven
- A token stored in a carried device such as a smart card or security token is used in conjunction with the reader to control access to areas of importance

Access Lists

- All secure entry points should have a readily available access list providing the permitted personnel and a black list, if applicable

- The use of a black list can aid in the apprehension of suspects

Proper Lighting

- Having well lit areas near access points can provide aid to cameras and guards alike

- Intruders often use dark areas as cover from critical security controls to avoid detection

- All building entrances and windows should have a source of lighting in near proximity

- Should be combined with dogs, CCTV or guards

Signs

- Warning signs provide a layer of security with notification of prohibited access or briefly outlining site information
- Can be used to declare areas as off limits
- Used as a deterrent

Guards

- All physical security controls, whether static deterrents or active detection and surveillance mechanisms, ultimately rely on personnel to intervene and stop actual intrusions and attacks

- Security guards exist to fulfill this need

- Post around perimeter, inside or both to monitor access points or maintain surveillance equipment

- The real benefit of guards is that they are able to adapt and react to various conditions or situations

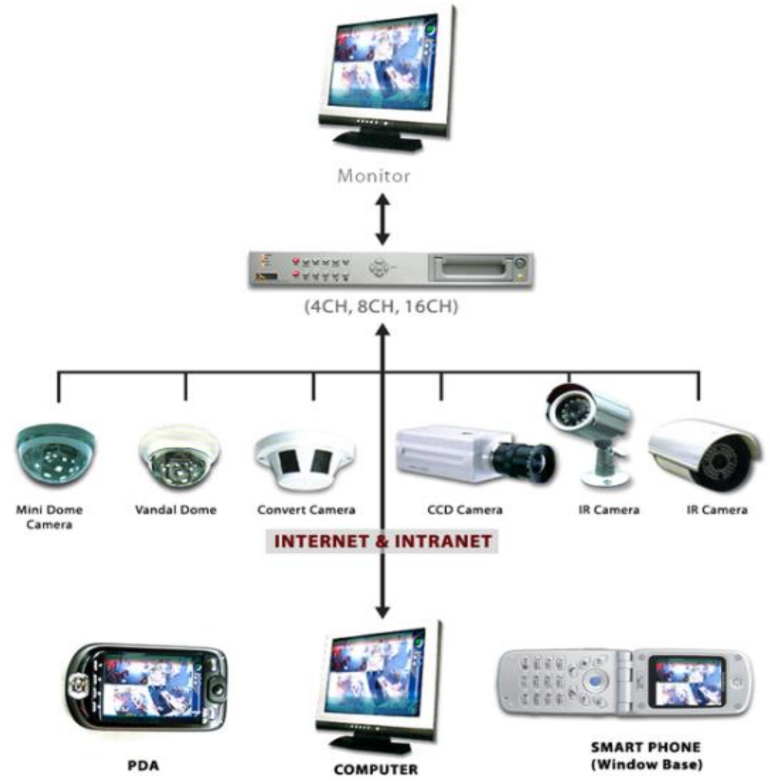
Barricades

- In addition to fencing, are used to control both foot traffic and vehicles

- K-rails (normally used in road construction, large planters, zigzag queues, bollards, and tire shredders are all examples

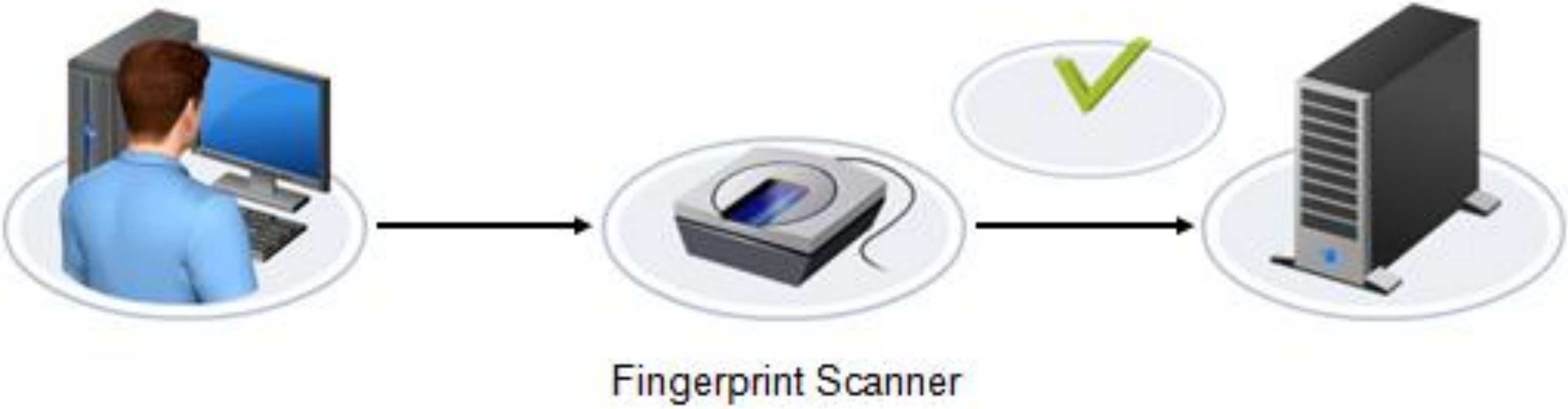
Video Surveillance

- Closed Circuit Television (CCTV)
- Often many different cameras networked together



Biometrics

- Based on an individuals’ physical characteristics
- Who you ARE



Biometrics

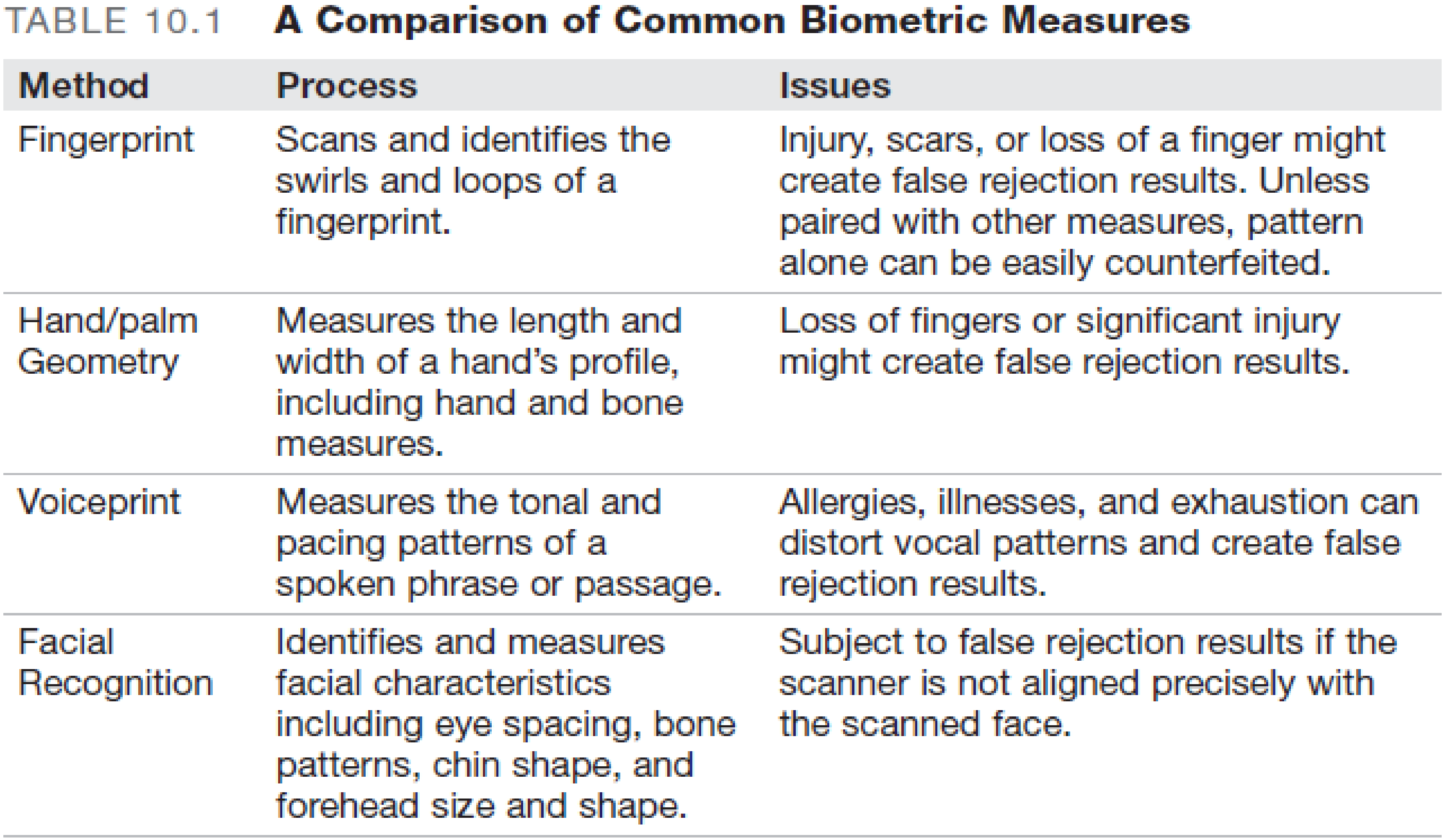


TABLE 10.1 **A Comparison of Common Biometric Measures**

Method	Process	Issues
Fingerprint	Scans and identifies the swirls and loops of a fingerprint.	Injury, scars, or loss of a finger might create false rejection results. Unless paired with other measures, pattern alone can be easily counterfeited.
Hand/palm Geometry	Measures the length and width of a hand's profile, including hand and bone measures.	Loss of fingers or significant injury might create false rejection results.
Voiceprint	Measures the tonal and pacing patterns of a spoken phrase or passage.	Allergies, illnesses, and exhaustion can distort vocal patterns and create false rejection results.
Facial Recognition	Identifies and measures facial characteristics including eye spacing, bone patterns, chin shape, and forehead size and shape.	Subject to false rejection results if the scanner is not aligned precisely with the scanned face.

Biometrics

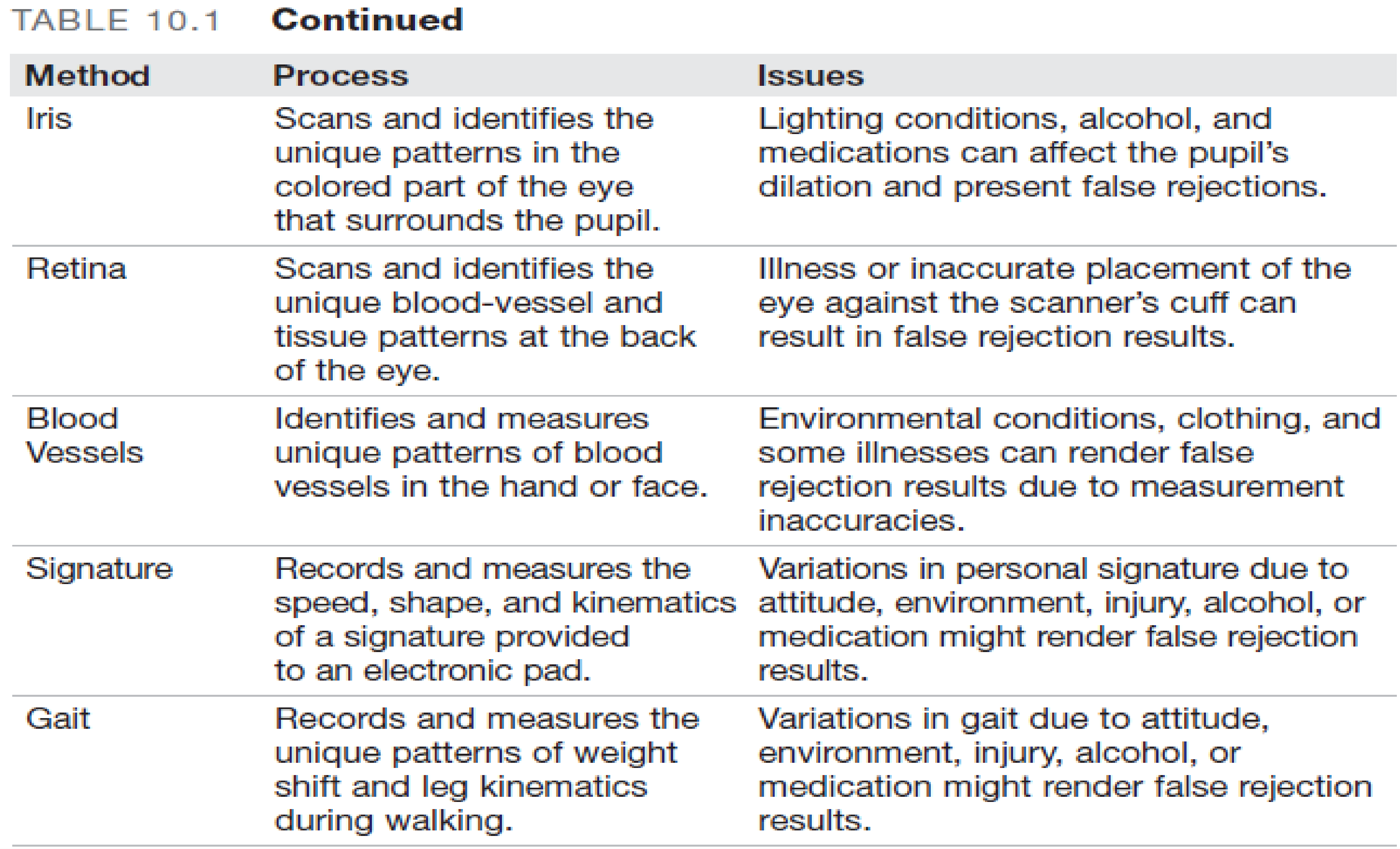


TABLE 10.1 **Continued**

Method	Process	Issues
Iris	Scans and identifies the unique patterns in the colored part of the eye that surrounds the pupil.	Lighting conditions, alcohol, and medications can affect the pupil's dilation and present false rejections.
Retina	Scans and identifies the unique blood-vessel and tissue patterns at the back of the eye.	Illness or inaccurate placement of the eye against the scanner's cuff can result in false rejection results.
Blood Vessels	Identifies and measures unique patterns of blood vessels in the hand or face.	Environmental conditions, clothing, and some illnesses can render false rejection results due to measurement inaccuracies.
Signature	Records and measures the speed, shape, and kinematics of a signature provided to an electronic pad.	Variations in personal signature due to attitude, environment, injury, alcohol, or medication might render false rejection results.
Gait	Records and measures the unique patterns of weight shift and leg kinematics during walking.	Variations in gait due to attitude, environment, injury, alcohol, or medication might render false rejection results.

Protected distribution (cabling)

- Protected distribution or protective distribution systems (PDSs) are the means by which cables are protected against unauthorized access or harm

- Used to deter violations, detect access attempts, and prevent compromise of cables

Alarms

- IDSs are systems designed to detect an attempted intrusion, breach or attack
- Physical IDSs, known as burglar alarms, detect unauthorized activities and notify the authorities
- Useful only if it is connected to an intrusion alarm
- Battery backups with enough stored power for 24 hours of operation is a must

Alarm Types

- Deterrent Alarms may engage additional locks or shut doors in efforts to increase intrusion difficulty

- Repellant Alarms usually sound an audio siren or bell and turn lights on

- Notification Alarms are often silent to the intruder, but record data about the incident and notify administrators, security and law enforcement

Alarm Systems

- Local Alarm System must broadcast an audible (up to 120 decibel [db]) alarm signal that can be easily heard up to 400 feet away

- Central Station System usually silent locally, but offsite monitoring agents are notified so they can respond to the security breach

- Auxiliary Station System can be added to either local or centralized alarm systems where it notifies emergency services

Motion Detection

- A motion detector, or motion sensor, is a device that senses movement or sound in a specific area

Motion Detection Types

- Infrared - Changes in the infrared lighting patterns

- Heat-based - Changes in the heat levels and patterns

- Wave-pattern – Emits a consistent low-frequency ultrasonic signal and monitors changes to the reflective patterns

- Capacitance - Changes in the electrical or magnetic field surrounding a monitored object

- Photoelectric - Changes in visible light levels

- Passive audio - Listens for abnormal sounds

Control Types

- Deterrent - discourage violation of security policies

- Preventive - thwart or stop unwanted or unauthorized activity from occurring

- Detective - discover or detect unwanted or unauthorized activity

- Compensating - provide various options to other existing controls to aid in enforcement and support of security policies

Control Types

- Corrective - returns the systems to normal after an unwanted or unauthorized activity
- Recovery - extension of corrective controls but have more advanced or complex abilities such as backup and restore
- Directive - direct, confine, or control the actions of subjects to force or encourage compliance with security policies
- Technical - hardware or software mechanisms used to manage access and to provide protection for resources and systems
- Administrative - policies and procedures defined by an organization’s security policy and other regulations or requirements

Student Check

What is the proper humidity level or range for IT environments?

○ A. Below 40 percent
○ B. 40 percent to 60 percent
○ C. Above 60 percent
○ D. 20 percent to 80 percent

Student Check

What is the proper humidity level or range for IT environments?

○ A. Below 40 percent

○ B. 40 percent to 60 percent

○ C. Above 60 percent

○ D. 20 percent to 80 percent

Student Check

Which of the following is a security control type that is not usually associated with or assigned to a security guard?

○ **A. Preventive**
○ **B. Detective**
○ **C. Corrective**
○ **D. Administrative**

Student Check

Which of the following is a security control type that is not usually associated with or assigned to a security guard?

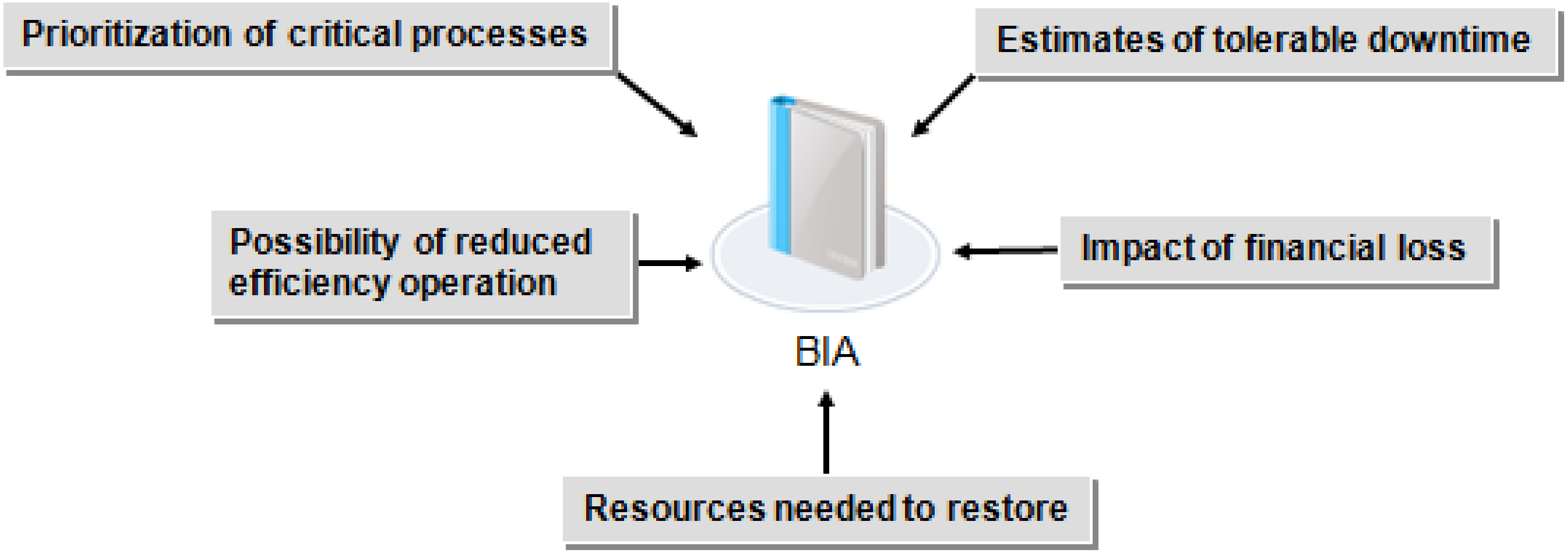
○ A. Preventive
○ B. Detective
○ C. Corrective
○ D. Administrative

Objective 2.8

- Compare and Contrast Aspects of Business Continuity

Business Impact Analysis (BIA)

- Focuses on the relative impact on critical business functions due to the loss of operational capability due to threats

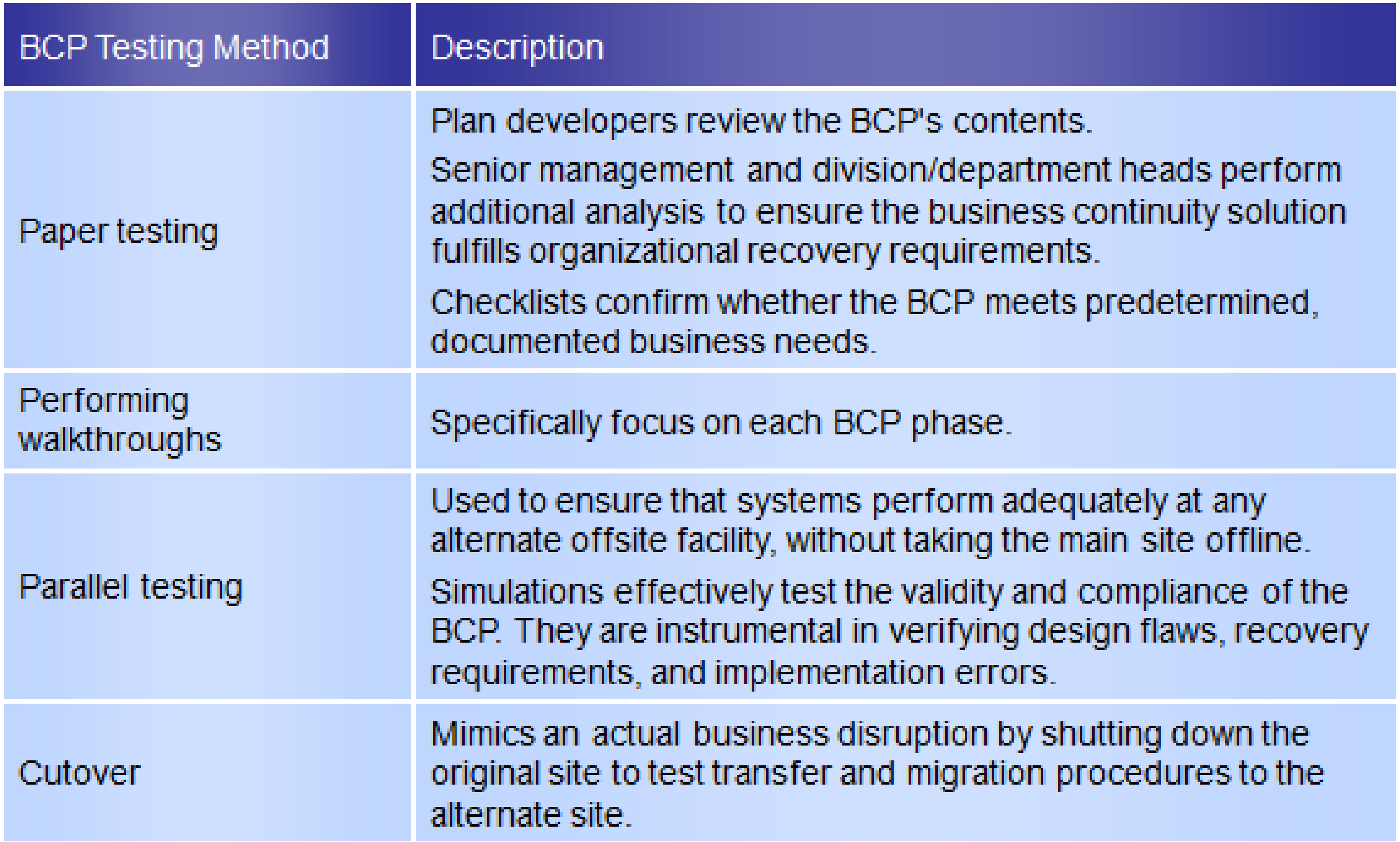

Prioritization of critical processes
Estimates of tolerable downtime
Possibility of reduced efficiency operation
Impact of financial loss
BIA
Resources needed to restore

Business Continuity Plan (BCP)

- Details the procedures to follow to reestablish proper connectivity and the facilities needed to restore data in the event of a catastrophic loss
- Remove single points of failure
  - **Items of consideration include network connectivity, facilities, clustering, and fault tolerance**

Business Continuity Planning and Testing

Top Priority of BCP and DRP is ALWAYS People



BCP Testing Method	Description
Paper testing	Plan developers review the BCP's contents. Senior management and division/department heads perform additional analysis to ensure the business continuity solution fulfills organizational recovery requirements. Checklists confirm whether the BCP meets predetermined, documented business needs.
Performing walkthroughs	Specifically focus on each BCP phase.
Parallel testing	Used to ensure that systems perform adequately at any alternate offsite facility, without taking the main site offline. Simulations effectively test the validity and compliance of the BCP. They are instrumental in verifying design flaws, recovery requirements, and implementation errors.
Cutover	Mimics an actual business disruption by shutting down the original site to test transfer and migration procedures to the alternate site.

Continuity of Operations (CooP)

- The component of the BCP that provides best practices to mitigate risks, and best measure to recover from the impact of an incident
  - Think day-to-day operations
  - High availability
  - Fault tolerance
  - Server clustering

Disaster Recovery Plan (DRP)

- A plan that prepares an organization to react appropriately if the worst were to happen

- Implemented when the BCP fails and the business stops

IT contingency planning

- Component of the Business Continuity Plan (BCP) that specifies alternate IT contingency procedures that you can switch over to when you are faced with an attack or disruption of service leading to a disaster for an organization

Succession planning

- Ensures that all key business personnel have one or more designated back-ups who can perform critical functions when needed

- Implemented when the person in charge goes down or is permanently unavailable

High Availability

- Maintaining an onsite stash of spare parts can reduce downtime
- Have a backup generator or UPS
- Strive to achieve the 5 “9s”

Redundancy

- RAID on Hard Drives
- Hot-swapping of failed drives and redundant power supplies so that replacement hardware can be installed without ever taking the server offline

Redundancy

- Hot Rollover – Automatic failover
- Cold Rollover – Manual failover

- Failsecure – resort to secure state
- Failsafe – human safety is protected
- Failsoft – only the failed portions are secured, while the rest of the system continues to function normally
- Failopen – resort to an unsecure state
- Failclosed – automatically locks and wont open

Tabletop Exercises

- A tabletop exercise is a discussion meeting focused on a potential emergency event

- Essentially a walk through and evaluation of an emergency plan in a stress-free environment

- Also called a “Structured Walkthrough”

Fault Tolerance

- Fault tolerance is the ability of a system to smoothly handle or respond to failure

- Can be software, hardware or backup power solutions

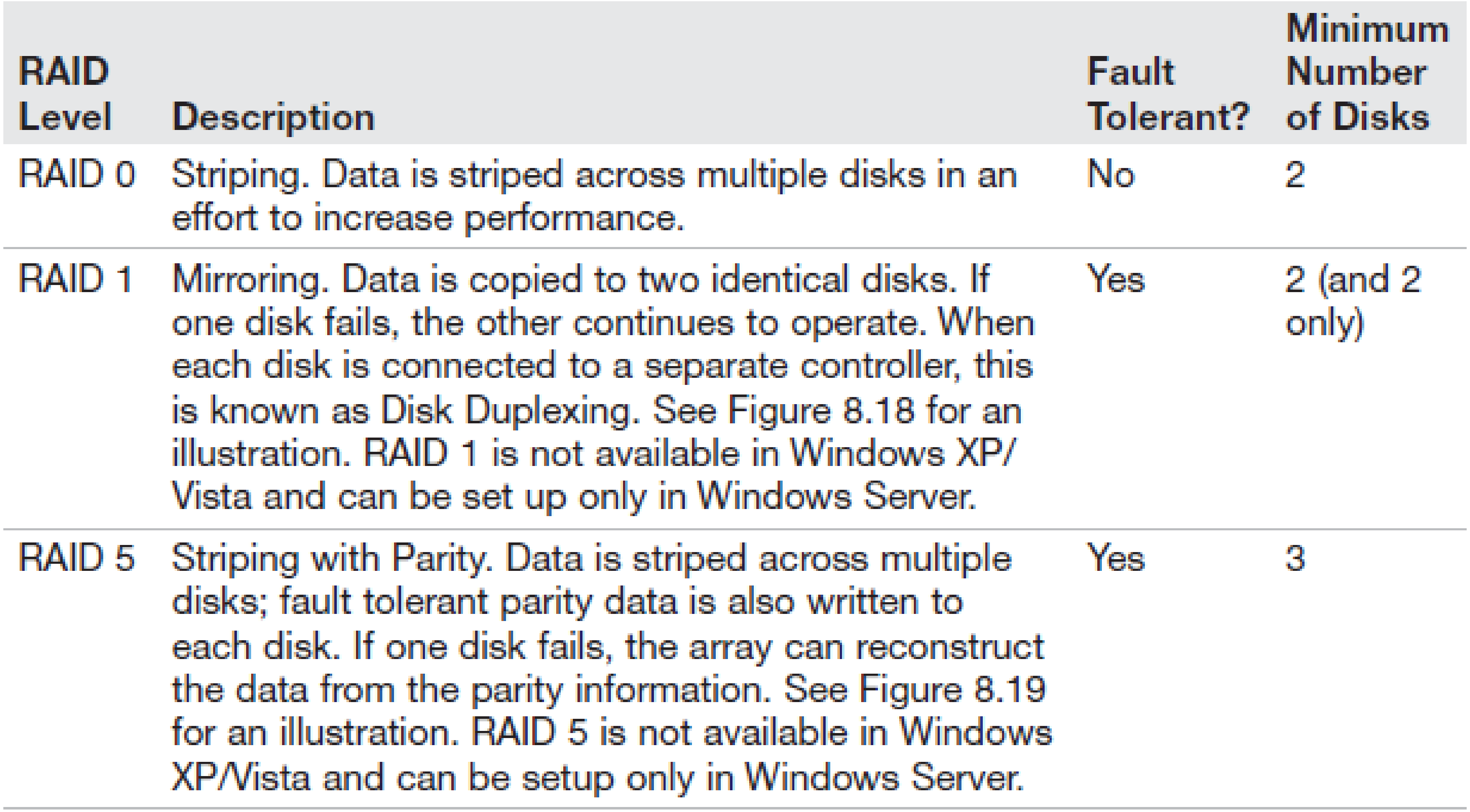
Hardware

- Any element in your IT infrastructure, component in your physical environment, or person on your staff can be a single point of failure

- To avoid single points of failure, you should design your networks and your physical environment with redundancy and backups by doing such things as deploying dual network backbones

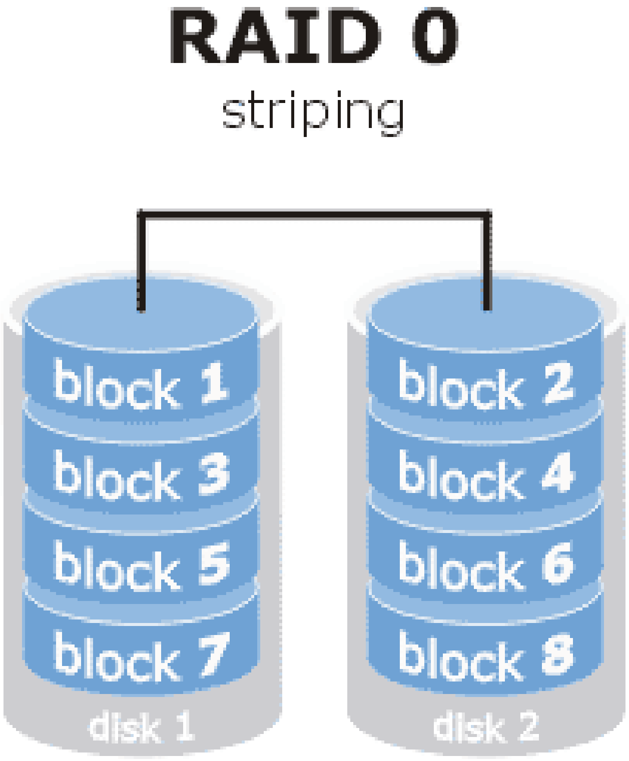
- Using systems, devices, and solutions with fault-tolerant capabilities improve resistance to single-points-of-failure vulnerabilities

RAID

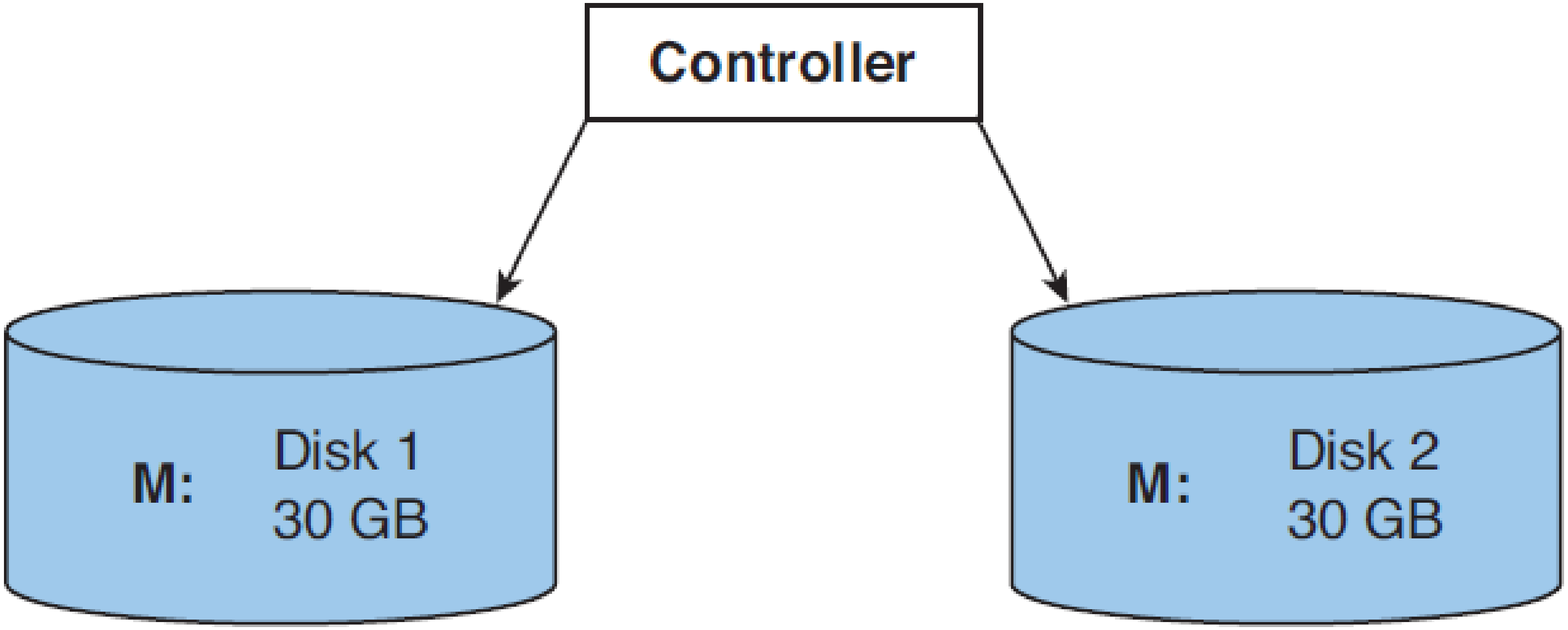


RAID Level	Description	Fault Tolerant?	Minimum Number of Disks
RAID 0	Striping. Data is striped across multiple disks in an effort to increase performance.	No	2
RAID 1	Mirroring. Data is copied to two identical disks. If one disk fails, the other continues to operate. When each disk is connected to a separate controller, this is known as Disk Duplexing. See Figure 8.18 for an illustration. RAID 1 is not available in Windows XP/ Vista and can be set up only in Windows Server.	Yes	2 (and 2 only)
RAID 5	Striping with Parity. Data is striped across multiple disks; fault tolerant parity data is also written to each disk. If one disk fails, the array can reconstruct the data from the parity information. See Figure 8.19 for an illustration. RAID 5 is not available in Windows XP/Vista and can be setup only in Windows Server.	Yes	3

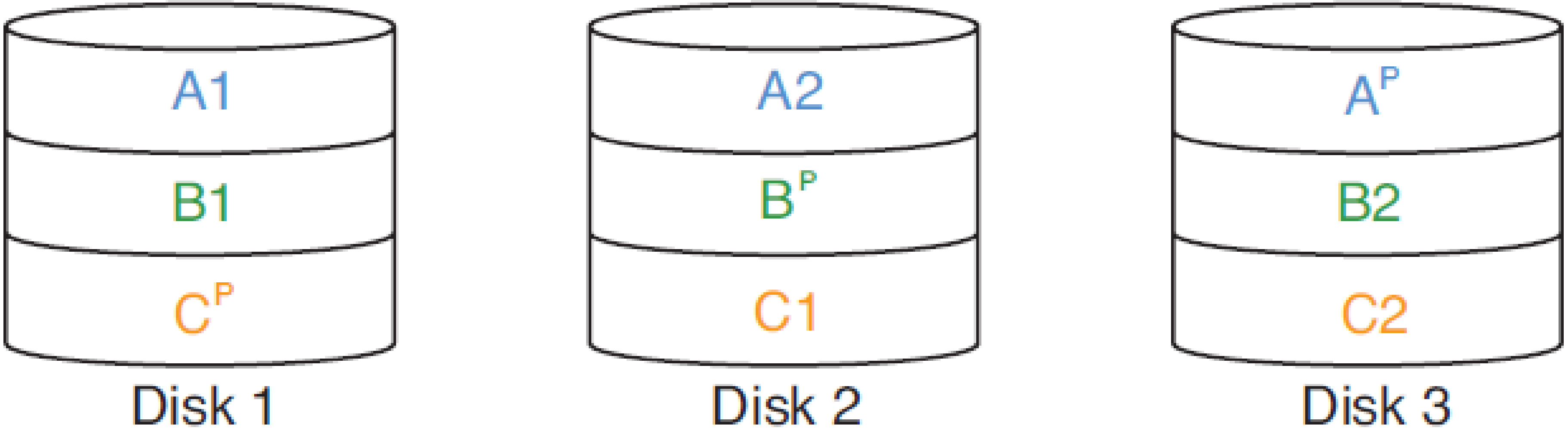
RAID 0- Stripe



RAID 1- Mirror



RAID 5- Striping with Parity



Clustering

- Clustering means deploying two or more duplicate servers in such a way as to share the workload of a mission-critical application

- A cluster controller manages traffic to and among the clustered systems to balance the workload across all clustered servers

Load Balancing

- A load balancer is used to spread or distribute network traffic load across several network links or network devices

- Covered in section 1.1

Servers

- Redundant servers are another example of avoiding single points of failure

- A redundant server is a mirror or duplicate of a primary server that receives all data changes immediately after they are made on the primary server

- A mirror server can take over and replace the primary in the event of a failure

Backup Techniques and Practices

- Fundamental to any disaster recovery plan is the need to provide for regular backups of key information, including user file and email storage; database stores; event logs; and security principal details such as user logons, passwords, and group membership assignments

- Without a regular backup process, loss of data through accidents or directed attack could severely impair business processes

- Backups should be kept offline and offsite

- Archive bit – file flag that is turned on when there is a modification or change

Backup Types

Backup Type	Data Backed up	Backup Time	Restore Time	Storage Space
Full Backup	All Data	Slowest	Fastest	Highest
Differential Backup	New/Changed Data since last Full backup	Moderate	Fast	Moderate
Incremental Backup	New/Changed Data since last backup	Fastest	Slowest	Lowest

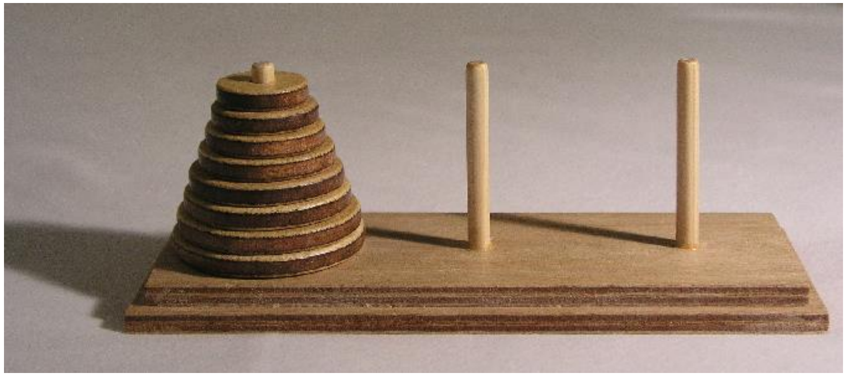
Backup Schemes

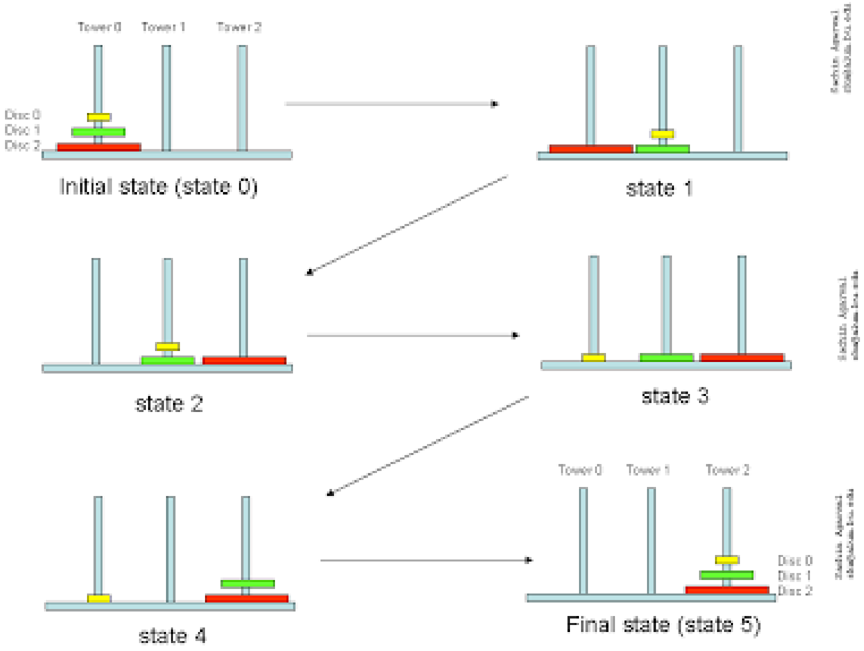
- Grandfather–Father–Son
- First set, “son,” represents daily backups.
- Second set, “father,” is used to perform full backups.
- Final set of three tapes, “grandfather,” is used to perform full backups on the last day of each month.
- Grandfather is monthly back-up stored off site
- Father is weekly back-up stored off site
- Son is daily back-up stored on site

Backup Schemes

Tower of Hanoi

This is a recursive method where every tape is associated with a disk in the puzzle, and the disk movement to a different peg corresponds with a backup to a tape.





Backup Schemes

Ten Tape Rotation

- Simpler and more cost-effective method for small
- businesses.

- **It provides a data history of up to two weeks.**

- Friday backups are full backups.

- Monday through Thursday backups are incremental.

Alternate sites

- Hot site
  - Location that is already running and available 24/7
  - Minimal downtime, but expensive
- Warm site
  - Scaled-down version of a hot site
  - Generally configured with power, phone, and network jacks
- Cold site
  - Merely a prearranged request to use facilities if needed
  - Cheapest option, but most downtime

Student Check

Which of the following is not a consideration for the business impact analysis?

○ **A. Identification of critical business functions**
○ **B. Identification of key services and technologies**
○ **C. Identification of likelihood of an incident**
○ **D. Identification of cost associated with an incident**

Student Check

Which of the following is not a consideration for the business impact analysis?

○ A. Identification of critical business functions

○ B. Identification of key services and technologies

○ C. Identification of likelihood of an incident

○ D. Identification of cost associated with an incident

Student Check

When is business continuity needed?

○ **A. When new software is distributed**
○ **B. When business processes are interrupted**
○ **C. When a user steals company data**
○ **D. When business processes are threatened**

Student Check

When is business continuity needed?

○ A. When new software is distributed

○ B. When business processes are interrupted

○ C. When a user steals company data

○ D. When business processes are threatened

Student Check

Which of the following is not a reason for activating succession plans?

○ A. Retraining
○ B. Death
○ C. Retirement
○ D. Injury

Student Check

Which of the following is not a reason for activating succession plans?

○ A. Retraining

○ B. Death

○ C. Retirement

○ D. Injury

Student Check

Which recovery site has only power, telecommunications, and networking active all the time?

○ A. Hot site
○ B. Cold site
○ C. Warm site
○ D. Shielded site

Student Check

Which recovery site has only power, telecommunications, and networking active all the time?

○ A. Hot site
○ B. Cold site
○ C. Warm site
○ D. Shielded site

Student Check

Which type of fault-tolerant RAID configuration provides the lowest disk usage fraction?

- ○ A. RAID 0
- ○ B. RAID 3
- ○ C. RAID 1
- ○ D. RAID 5

Student Check

Which type of fault-tolerant RAID configuration provides the lowest disk usage fraction?

- ○ A. RAID 0
- ○ B. RAID 3
- ○ C. RAID 1
- ○ D. RAID 5

Student Check

Which of the following types of planning assists in preventing loss of service in the event of a server failure?

○ **A. Network connectivity**
○ **B. Facilities**
○ **C. Clustering**
○ **D. Fault tolerance**

Student Check

Which of the following types of planning assists in preventing loss of service in the event of a server failure?

○ A. Network connectivity

○ B. Facilities

○ C. Clustering

○ D. Fault tolerance

CIA Triad

- Security directives includes maintaining the **confidentiality, integrity, and availability** of data and services

- Threats to these three principles are constantly present and evolving

INTEGRITY
AVAILABILITY
CONFIDENTIALITY

- Defensive measures must be put into place to mitigate risk within the enterprise

Confidentiality

- Keeps information and communications private and protected from unauthorized access

- Includes data encryption, physical access controls, logical access controls, and security policies to protect against shoulder surfing, social engineering, and other forms of observational disclosure

- Encryption, Access controls, and Steganography

Integrity

- Keeps organization information accurate, free of errors and without unauthorized modifications

- Includes malware defenses protecting against data corruption or elimination, validation code that protects against code injection or malformed data input, data hashing, validation, identifying modifications, and limited user interface options controlling the types of access available to data

- Hashing, Digital Signatures, Certificates, and Non-repudiation

Availability

- Ensures systems operate continuously and that authorized persons can access the data that they need
- Includes load balancing systems, redundant services and hardware, backup solutions, and environmental controls intended to overcome outages affecting networking, power, system, and service outages

Non-Repudiation

- Supplemental to the CIA Triad
- Ensures that the party that sent a transmission or created data remains associated with that data

Safety

- Safety of the facility and personnel should always be the top priority of a security effort

- Fencing, lighting, locks, CCTV, escape plans, drills, escape routes, and testing controls are all areas of importance when concerning facility and personnel safety

Student Check

You run a full backup every Monday. You also run a differential backup every other day of the week.
You experience a drive failure on Friday.

Which of the following restoration procedures should you use to restore data to the replacement drive?

❍ A. Restore the full backup and then each differential backup
❍ B. Restore the full backup and then the last differential backup
❍ C. Restore the differential backup
❍ D. Restore the full backup

Student Check

You run a full backup every Monday. You also run a differential backup every other day of the week.
You experience a drive failure on Friday.

Which of the following restoration procedures should you use to restore data to the replacement drive?

- ○ **A. Restore the full backup and then each differential backup**
- ○ **B. Restore the full backup and then the last differential backup**
- ○ **C. Restore the differential backup**
- ○ **D. Restore the full backup**

Student Check

Which two of the following support the preservation of data availability?

- ○ A. Anti-static carpet
- ○ B. Firewall
- ○ C. Mirrored windows
- ○ D. Backups

Student Check

Which two of the following support the preservation of data availability?

- ○ A. Anti-static carpet
- ○ B. Firewall
- ○ C. Mirrored windows
- ○ D. Backups

Student Check

Encryption primarily supports which element of data security?

○ **A. Confidentiality**
○ **B. Integrity**
○ **C. Availability**
○ **D. Accuracy**

Student Check

Encryption primarily supports which element of data security?

- ○ A. Confidentiality
- ○ B. Integrity
- ○ C. Availability
- ○ D. Accuracy