

Security+ SY0-601

Module 5: Controls.

Part - 1



Table of Contents.

1 Information security

2 Administrative controls

3 Control categories and types

4 Physical security

5 Access controls

6 Privacy and sensitive data security

7 Authentication

8 Host security

9 Network security

10 Secure coding practices

Learning objectives.

Upon Completion of this module, you should be able to:

- Define the basics of information security and defense-in-depth concepts.
- Outline key administrative controls and explain their importance.
- Define the categories and types of controls. Differentiate between a category and a type with respect to controls.
- Describe how physical security defends a network. List physical controls and explain how they work.
- Explain models, methods, and roles in controlling access to data in various locations and forms.

CONTINUED ON NEXT SLIDE >

Learning objectives.

Upon Completion of this module, you should also be able to:

- Discuss aspects of privacy, data security, and roles and responsibilities for each.
- List the various authentication factors and provide examples of each. Explains the federation concepts, attestation, AAA servers, and directory services.
- List aspects of hardening various endpoint systems, including software, authentication, and configuration. Identify aspects to look at and to look for with respect to hardening.
- Explain the uses of network security appliances and services.
- Discuss aspects of secure coding, testing, debugging, and deployment.

Information Security.

INFORMATION SECURITY.

Information security.

In this section, we will cover the following key concepts:

- Security principles.
- The CIA triad.
- Defense-in-depth.
- Site resiliency.
- Diversity.



INFORMATION SECURITY.

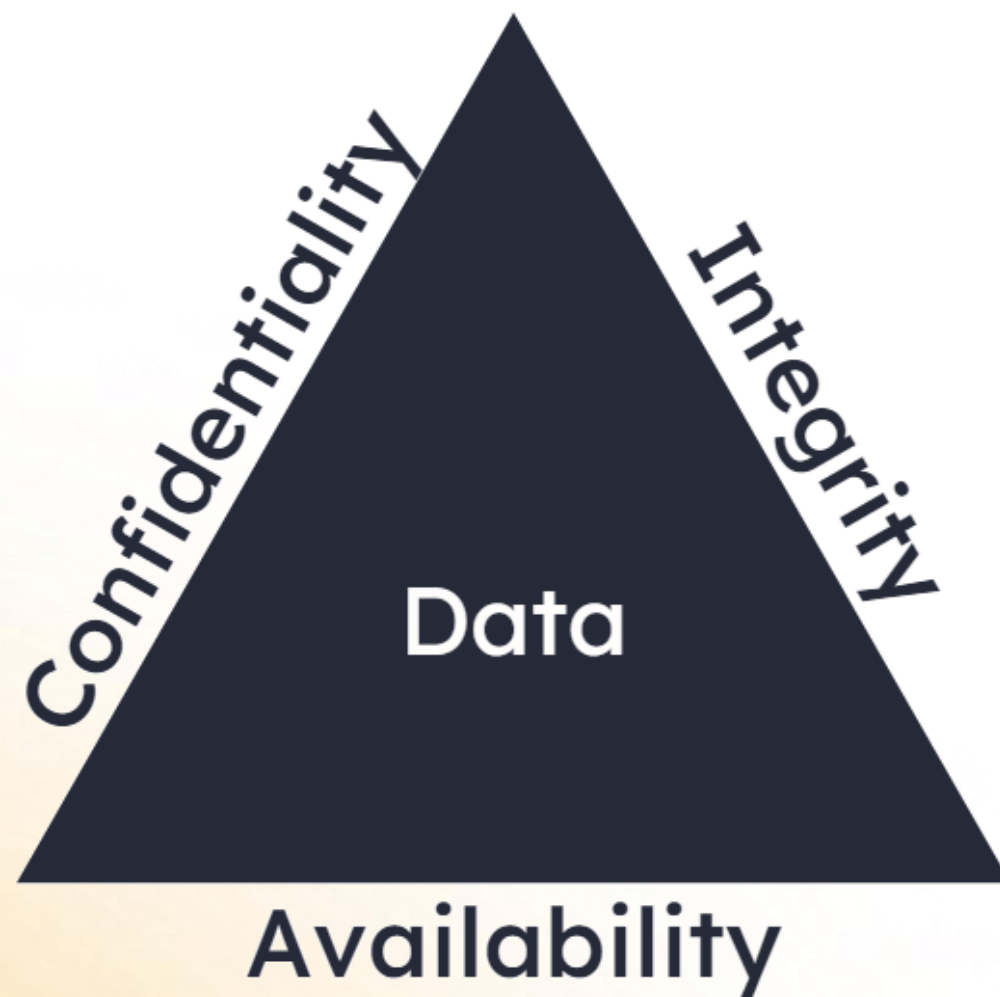
Security principles.



CIA (Confidentiality, Integrity, and Availability) are the foundations of successful security implementation in a network; these principles identify how we encrypt, hash, and otherwise audit our network resources to maintain security.

INFORMATION SECURITY.

The CIA triad.

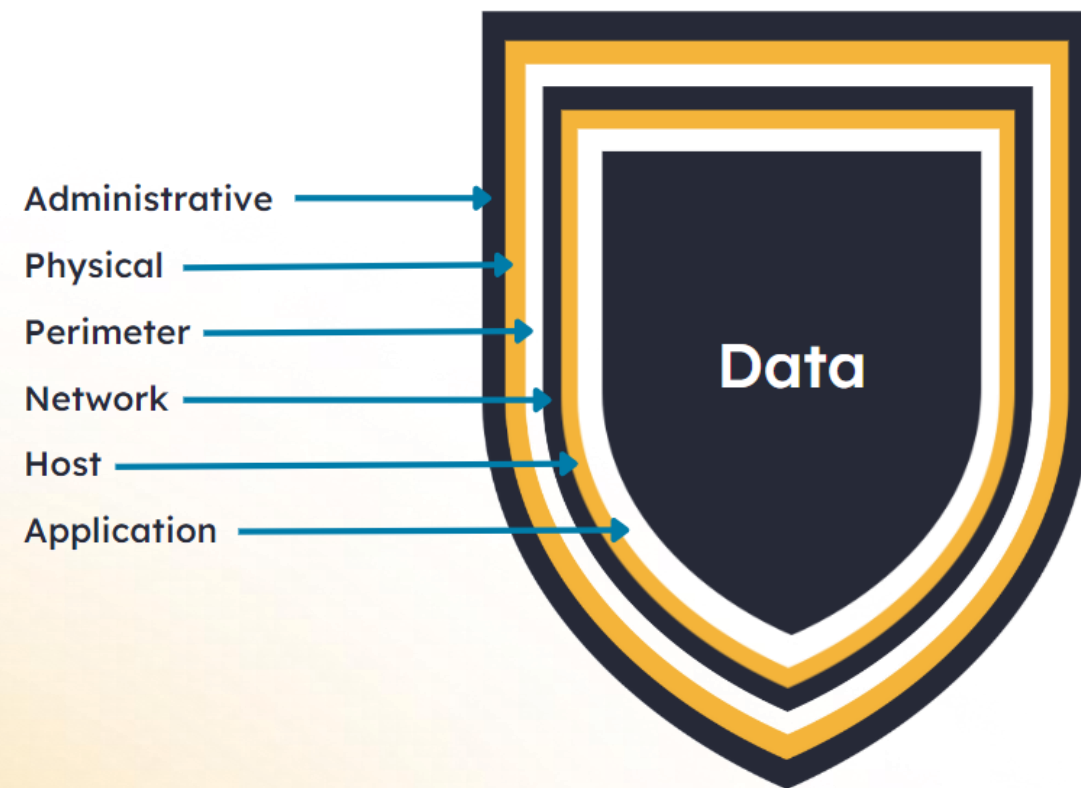


The CIA Triad represents the three primary goals of information security:

- Confidentiality
- Integrity
- Availability

INFORMATION SECURITY.

Defense-in-depth.



Defense-in-depth

Layered security

Defense-in-depth layers.

The **administrative layer** is comprised of aspects ranging from policies and procedures to permissions to monitoring and log analysis. Security principles and directives will also be addressed in this layer.

The **physical layer** includes onsite and offsite physical controls; it may include fencing, locks, fire extinguishers, authentication, data backups, and hot, warm, and cold sites.

The **perimeter layer** is the network perimeter, where defenses such as firewalls or an IDS/IPS may be placed to control inbound and outbound traffic.

The **network layer** encompasses defenses and controls focused on traffic moving through the internal network; it may include internal VPNs, switch port security, packet and traffic analysis, network sensors, internal routers, network firewalls, and NIDS/NIPS.

CONTINUED ON NEXT SLIDE >

Defense-in-depth layers.

The **host layer** is comprised primarily of settings and software. File permissions, firewalls, HIDS, VPN software, antivirus software, and external backup software may be contained in this layer.

The **application layer** includes applications that can be secured through configurations that limit access or control the permitted activities; this layer may protect data by scrubbing malicious input that might otherwise have gained access.

The **data layer** focuses on data protection through data encryption at rest and in transit. Hashes of files and backups may serve to maintain data integrity. Data may also be controlled through strong permissions. Homomorphic encryption may be used to share sensitive data enough to analyze it without exposing private information.

INFORMATION SECURITY.

Site resiliency.

Many enterprise-level organizations created multiple alternate processing or recovery sites:

Hot site. Failover can happen almost immediately. Data from the primary site must already be at this location.

Warm site. Failover happens quickly. Real-time data is not at these sites, so an updated data set will need to be provided.

Cold site. Failover does not happen quickly at all. These might simply be a space that the organization has purchased or rented. Everything must be procured, set up, and installed before data can be moved and operations resume.



INFORMATION SECURITY.

Diversity.

- Vendor diversity
- OS diversity
- Cryptographic diversity



INFORMATION SECURITY.

Other support items for information security.

Information about systems must be kept up-to-date for security professionals to be able to assess the security posture of the systems. The following types of documentation and schemas must be considered:

- Diagrams
- Baseline configuration
- Standard naming conventions
- Internet protocol (IP) schema

INFORMATION SECURITY.

Knowledge Check.

Let's apply what we have covered:

- Describe the different forms of security diversity.
- Describe defense-in-depth.



Administrative Controls.

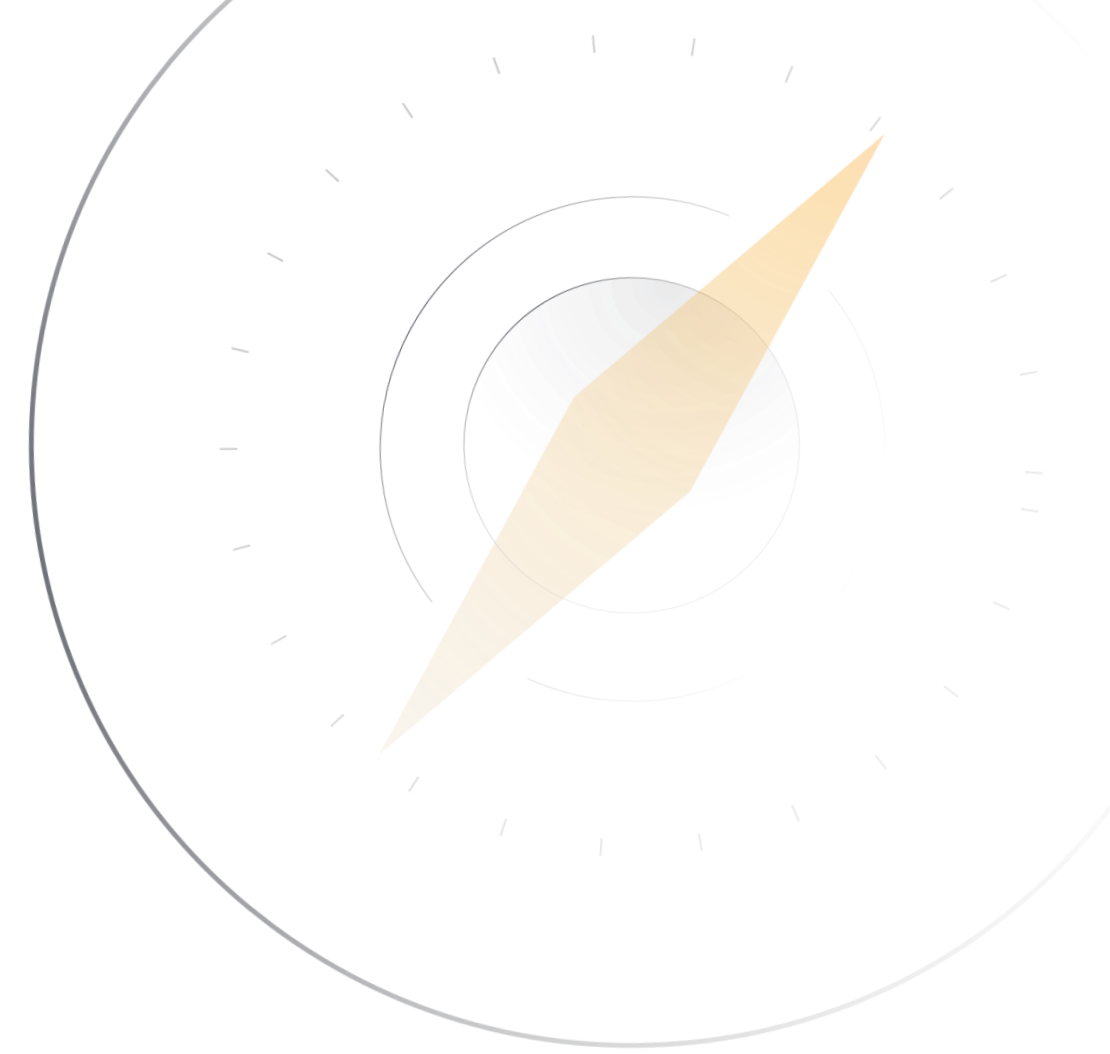


ADMINISTRATIVE CONTROLS.

Administrative controls.

In this section, we will cover the following key concepts:

- Laws, Regulations, and Policies.
- Standards, Procedures, Guidelines.
- Personnel Policies.
- Job Rotation.
- Separation of Duties.
- Non-Repudiation.
- Mandatory Vacations.
- Training.
- Data Policies.
- Credential Policies.
- Least Privilege.
- Organizational Policies.
- Account Policies.
- Location and Time Policies.



ADMINISTRATIVE CONTROLS.

Laws, regulations and policies.

Laws and **regulations** govern how a business conducts itself and stores private data. Every state has different laws and federal regulations regarding how to utilize IT services within an organization.

Policies are ways to ensure a company complies with laws and regulations. Organization standards come from higher-level policies.



ADMINISTRATIVE CONTROLS.

Standards, procedures, and guidelines.



Standards

Procedures

Guidelines

ADMINISTRATIVE CONTROLS.

Personnel policies.

- Acceptable use policy
- Clean desk policy
- Social media analysis
- Onboarding
- Offboarding

ADMINISTRATIVE CONTROLS.

Job rotation.



- **Job rotation** allows us to train employees on multiple job types to understand how certain security measures are implemented in the network.

- Job rotation allows a business to maintain continuity by way of employee knowledge. What happens with job rotation is that each employee knows just enough about another employee's job that, should something happen, they can at least keep that area of the business afloat until a replacement is found.

ADMINISTRATIVE CONTROLS.

Separation of Duties (SoD).



Separation of Duties (SoD) allows an organization to help prevent fraud and error by removing the aspect of repudiation.

SoD is a way to maintain integrity with our procedures.

You may work in an environment where one portion (or person) writes checks, then another portion (or person) signs and ships them; that is a direct reflection of SoD. Further, you may see in your networks that one person handles account security items while another maintains auditing on the same account.

ADMINISTRATIVE CONTROLS.

Nonrepudiation.



Nonrepudiation takes away the ability for a user to say they did not complete a task or complete a process by way of implementing firm auditing.

Nonrepudiation is the end goal when we audit portions of the business and monitor end users.

Nonrepudiation is often implemented through digital signatures.

ADMINISTRATIVE CONTROLS.

Mandatory vacations.



Mandatory vacation allows an organization to identify and prevent fraud by disabling user accounts during a timeframe to identify the source of malicious activity inside their network.

You will most likely see a company you work for initializing or enforcing a policy like a mandatory vacation; this helps identify if you have an employee doing "something shady" by taking them away from the network and identifying how things are run in their absence.

You may never actually implement this policy, but you may see it enforced where you work or possibly be told to take a vacation during an audit.

ADMINISTRATIVE CONTROLS.

Training.

Training is one of the most important aspects of security for an organization. Employees must be taught organizational policies and how to comply; they must have a firm grasp of their responsibilities to organizational security — this includes social engineering.

Additionally, specific training towards each employee's role in the organization should be addressed, which helps with retention and increased cross-training aids with security and succession planning.

CONTINUED ON NEXT SLIDE >



ADMINISTRATIVE CONTROLS.

Training.

Training should be diverse in nature, as no “one-size-fits-all” strategy is productive. Training should be based on roles and account for different learning styles.

Options for training include:

- Phishing campaigns.
- Capture the flag.
- Computer-based training.
- Gaming.
- Walkthroughs.
- One-on-one mentoring or coaching.



ADMINISTRATIVE CONTROLS.

Data policies.

A **data classification policy** established guidelines for classifying data based on its level of sensitivity, value, and criticality. Classifying data aids with security for data in transit, data at rest, and data in use and is important with data retention and storage; it also greatly aids Data Loss Prevention programs.

A **data governance policy** describes the security controls applied to data throughout its lifecycle.

A **data retention policy** helps the organization understand how long specific data must be retained to comply with various laws and regulations.

Credential policies.

User account types:

- **Standard user account** – This is the normal account type most users are provisioned; these accounts fall under normal account auditing policies.
- **Shared and generic accounts** – These should be used only sparingly, as a security professional cannot see who accessed the account at any time.
- **Guest accounts** – Best practices state that these accounts should be disabled. Guest accounts are useful for an anonymous login on a device that has access only to the internet; they are often used on kiosk-type computing devices.

CONTINUED ON NEXT SLIDE >

ADMINISTRATIVE CONTROLS.

Credential policies.

Service accounts – These are used by scheduled processes to run background processes. You do not log in using these accounts.

- **System** – Has the most privileges of any account in the Windows operating system. Any process created by this account has full access to anything on that computer.
- **Local service** – Has the same privileges as a standard user account; it accesses network resources as an anonymous user.
- **Network service** – Has the same privileges as a standard user account; it accesses network resources using the computer's account credentials.

CONTINUED ON NEXT SLIDE >

ADMINISTRATIVE CONTROLS.

Credential policies.

Privileged accounts – Have extra permissions to make configuration changes to a system, including the administrator and/or root accounts.

Third-party credentials are used to manage a vendor service or cloud applications; these are often used with APIs or as a login using SSH.

ADMINISTRATIVE CONTROLS.

Least privilege.



- The **least privilege** principle allows us to prevent privilege escalation by providing users with only the privileges they need to accomplish their jobs — nothing more.
- The least privilege principle is organization-wide. When personnel change jobs or are promoted, their security privileges must be evaluated; do not simply “add” more — match the privileges with the job responsibilities.

Organizational policies.

Change management is a deliberate implementation plan and also requires each change to have a remediation or rollback plan should the change negatively affect the system.

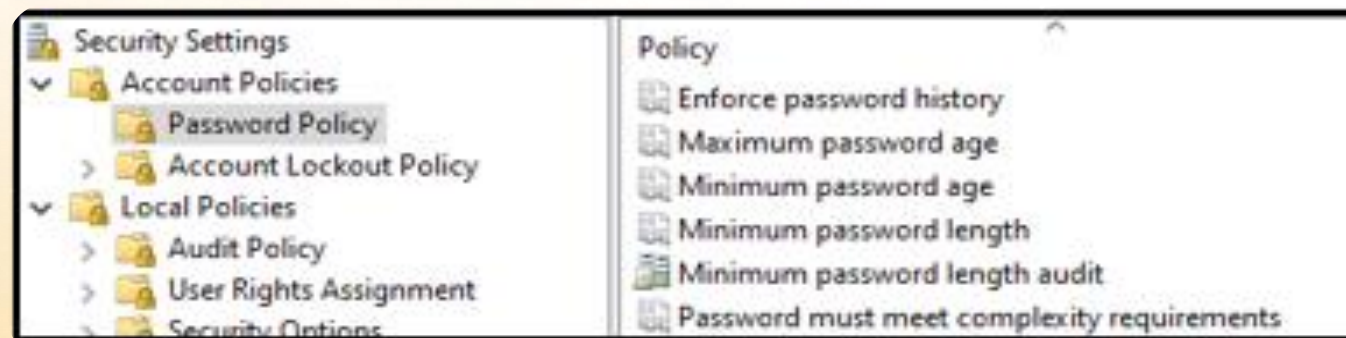
Change control is a process in which a proposed change is submitted, in writing, to the CAB (change advisory board) for consideration. Each change is reviewed, a decision is made on whether and when to move forward, and a communications plan is created.

Asset management refers to having an up-to-date inventory of all assets and the configuration settings for each device.

ADMINISTRATIVE CONTROLS.

Account policies.

Account policies are in place in a secured computing environment to ensure that only authenticated and authorized users can log into a system.



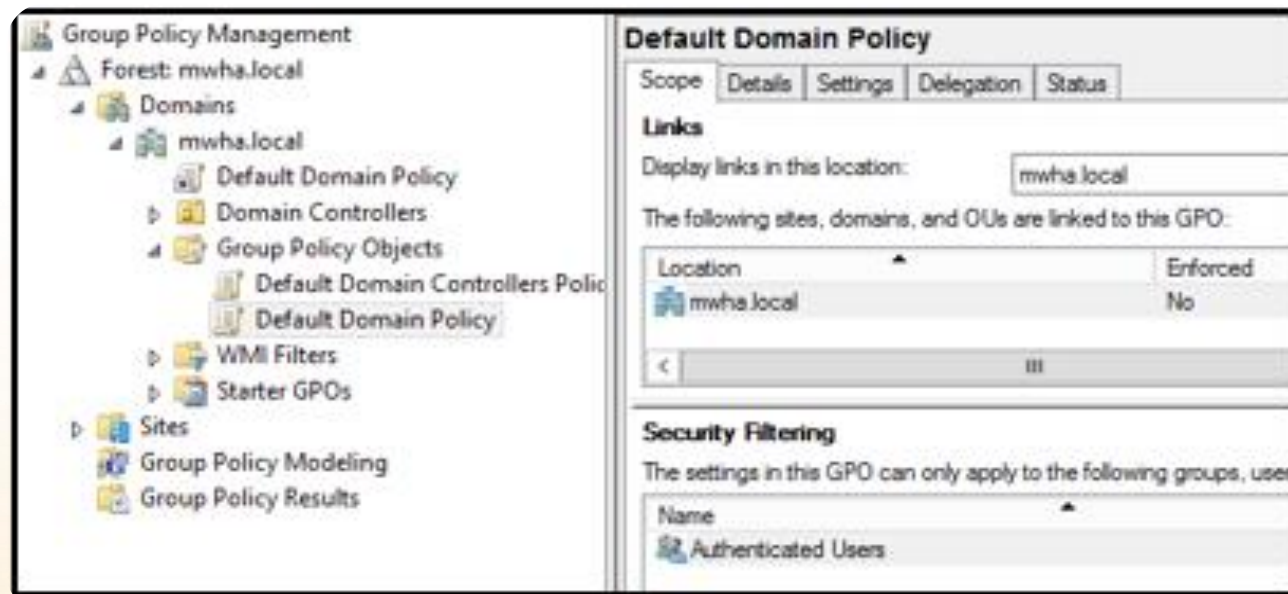
The following policies assist with credential management principles through the use of password requirements such as:

- **Minimum password length** – Enforces a minimum length for passwords.
- **Password complexity** – Specifies if complex passwords are required. A complex password has a mix of upper- and lower-case characters, numbers, and special characters.
- **Password history** – Enforces the maximum number of past passwords remembered, generally 12-24; this minimizes password reuse.
- **Minimum password age** – Specifies the fewest number of days a password must be kept; this also minimizes password reuse.
- **Maximum password age** – Specifies the longest number of days a password must be kept.

CONTINUED ON NEXT SLIDE >

ADMINISTRATIVE CONTROLS.

Account policies.



Additional attributes that can be used to assist with accounts and devices:

Access policies – Determine if an account can log onto a system, have access to a file, log on locally or via a domain, etc. Access policies can be implemented in Active Directory using Group Policy Objects (GPO).

Account permissions – Security professionals must always audit accounts to ensure “permission creep” has not allowed an account to obtain too many permissions over several years as the account holder is promoted.

Account audits – A process to determine whether an account is at risk, compromised, or being misused. In Windows, the Security Log in Event Viewer will show Audit Failures or Audit Successes.

ADMINISTRATIVE CONTROLS.

Location and time policies.

Additional attributes that can be used based on location and time:

Geofencing – Uses location as an attribute in the access request evaluation.

Geotagging – Adds geolocation metadata to files or devices; this data can be added into asset management software.

Geolocation – Users and devices can be located using IP addresses or location services such as GPS.

Time of day – Authorized logon hours for an account.

CONTINUED ON NEXT SLIDE >

ADMINISTRATIVE CONTROLS.

Location and time policies.

Additional attributes that can be used based on location and time:

Time-based logins – Maximum number of hours an account may be logged in.

Impossible travel time/risky login – Tracks the location of login events over a period of time. Accounts can be disabled if restrictions are not met; for example, a login happens from a device in Washington, DC, at 10:00 am UTC and then again from Seattle at 11:00 am UTC — since this cannot physically happen, the account is disabled.

ADMINISTRATIVE CONTROLS.

Knowledge Check.

Let's apply what we have covered:

- Describe the separation of duties.
- Why is job rotation important?



Control Categories and Types.



CONTROL CATEGORIES AND TYPES.

Control categories and types.



In this section, we will cover the following key concepts:

- Control Categories:
 - Technical.
 - Operational.
 - Managerial.
- Control Types:
 - Preventative.
 - Detective.
 - Corrective.
- Additional Controls:
 - Physical.
 - Deterrent.
 - Compensating.

CONTROL CATEGORIES AND TYPES.

Control categories.

A **control category** is simply a way of broadly grouping controls and categorizing them by how they are implemented.

① Technical controls

② Operational controls

③ Managerial controls

Technical control.



Technical controls are implemented as a system or part of a system, including hardware, software, and firmware.

Technical controls are implemented in a network to secure it, utilizing technology. Firewalls, IPS, and multi-factor authentication technologies are used to secure a network.

CONTROL CATEGORIES AND TYPES.

Operational control.



- **Operational controls** are identified by the fact that people implement them. Think of them as instructions followed by personnel.
- Operational controls are implemented in a network to secure it, utilizing people to make it happen.

CONTROL CATEGORIES AND TYPES.

Managerial control.



- **Managerial controls** oversee the information system, identifying details on which decisions can be made.

- A risk assessment and vulnerability scan, used to assess or provide a return on investment analysis of technical controls, are examples of managerial controls; other examples include rules and regulations for system access, access control, and automation of processes.

CONTROL CATEGORIES AND TYPES.

Control categories.



Security control is designed to provide or increase confidentiality, integrity, and availability; ideally, it includes efforts to tie a person's actions to that person beyond dispute, a principle known as nonrepudiation.

CONTROL CATEGORIES AND TYPES.

Security control functional types.



Security controls are often grouped by how they function or by the goal they seek. Note that some controls fit in more than one of the following types:

- Preventative
- Detective
- Corrective
- Physical
- Compensating
- Deterrent

Preventative controls.

Security control functional types:

- Preventative
- Detective
- Corrective
- Physical
- Compensating
- Deterrent

Preventive controls seek to reduce or eliminate the possibility that a particular attack or other threat can successfully occur. In other words, they attempt to stop something before it happens.

CONTROL CATEGORIES AND TYPES.

Detective controls.

Security control functional types:

- Preventative
- **Detective**
- Corrective
- Physical
- Compensating
- Deterrent

Detective controls are implemented into a network to send some alert of an issue after it has happened or while it is in progress.



CONTROL CATEGORIES AND TYPES.

Corrective controls.

Security control functional types:

- Preventative
- Detective
- **Corrective**
- Physical
- Compensating
- Deterrent

Where preventive controls attempt to reduce or eliminate the probability of an attack before it occurs, **corrective controls** seek to reduce or eliminate the impact of repeat attacks.

Corrective controls are implemented into a network to try and mitigate damage from a cyber-attack.



CONTROL CATEGORIES AND TYPES.

Physical controls.

Security control functional types:

- Preventative
- Detective
- Corrective
- **Physical**
- Compensating
- Deterrent

Physical controls include anything that aims to prevent, detect, or deter access to premises or hardware, which extends to alarms, lighting, and cameras.

CONTROL CATEGORIES AND TYPES.

Compensating controls.

Security control functional types:

- Preventative
- Detective
- Corrective
- Physical
- **Compensating**
- Deterrent

Compensating controls make up for the lack of proper control, as when a legacy system for which patches are no longer forthcoming is placed in a highly defensible subnet to make up for the unpatchable vulnerabilities.

CONTROL CATEGORIES AND TYPES.

Deterrent controls.

Security control functional types:

- Preventative
- Detective
- Corrective
- Physical
- Compensating
- Deterrent

Deterrent controls seek to discourage an attacker from proceeding, often indicating greater risk and smaller payoff; examples include signage, highly visible cameras, well-lit parking lots, fences, guard dogs, etc.

Technical controls by function type.

	Preventative	Detective	Corrective	Physical	Deterrent	Compensating
ACLs	✓					✓
Alarms		✓		✓	✓	
Antivirus software	✓			✓		
Auditing		✓			✓	
Authentication	✓					
CCTV		✓		✓	✓	
Encryption	✓					
Firewalls	✓					✓
IDS		✓				
IPS	✓					
Mantrap	✓			✓	✓	
Motion detectors		✓		✓		
Warning banners				✓	✓	

Operational controls by function type.

	Preventative	Detective	Corrective	Physical	Deterrent	Compensating
Backup rotations			✓			
Badges	✓			✓		
Dogs	✓	✓		✓	✓	
Hot/Warm/Cold sites			✓			✓
Job rotation		✓			✓	✓
Lighting				✓	✓	
Personnel procedures	✓				✓	
Training	✓		✓			✓
Security guards	✓	✓		✓	✓	
Security policies	✓		✓		✓	
Separation of duties	✓					
Termination			✓		✓	

Managerial controls by function type.

	Preventative	Detective	Corrective	Physical	Deterrent	Compensating
Alarms		✓		✓		✓
Auditing		✓			✓	
Background checks	✓					
Job rotation	✓		✓			
Network monitoring		✓			✓	
Non-repudiation		✓			✓	
Risk assessments			✓			
Security policies	✓		✓		✓	
Security reviews			✓			
Separation of duties	✓		✓			
SIEM		✓				
SNMP		✓	✓			
Supervision		✓	✓		✓	

CONTROL CATEGORIES AND TYPES.

Knowledge Check.

Let's apply what we have covered:

- Describe the differences between a control category and a control type.
- Describe preventative and detective control types.



Physical Security.

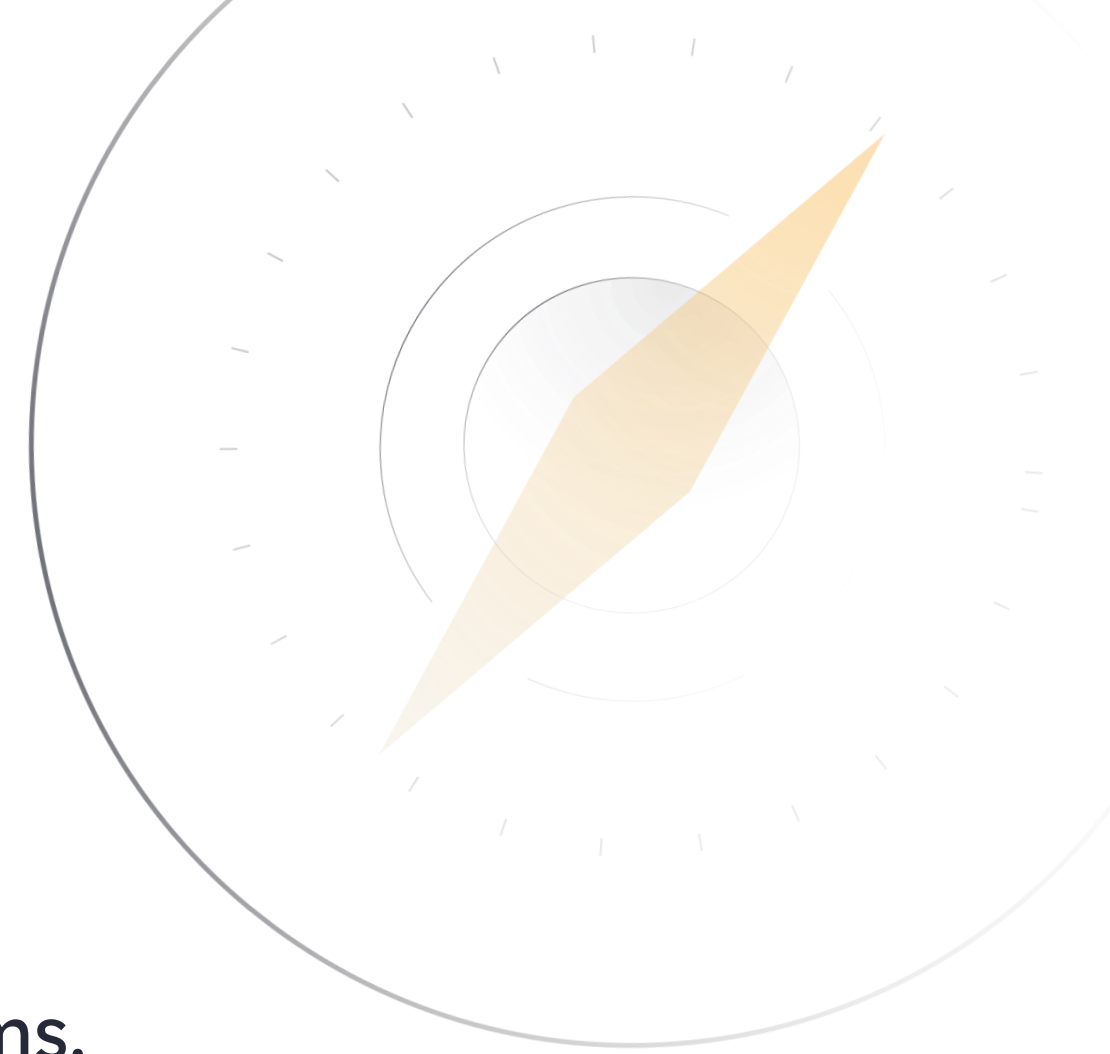


PHYSICAL SECURITY.

Physical security.

In this section, we will cover the following key concepts:

- Facility Security.
- Secure Areas.
- Video Surveillance and Security Personnel.
- Locks.
- Sensors and Alarms.
- Secure Data Destruction.
- Physical Data Security.
- Fire Suppression.



PHYSICAL SECURITY.

Physical security.

Physical security is about defenses of a physical nature; they defend physical access to premises, property, and personnel.

Industrial camouflage involves preventing a potential attacker from observing defenses from a distance by raising barriers to visibility; this could take the form of a wall that blocks the view of the front doors, cameras, turnstiles, and guard desks.

CONTINUED ON NEXT SLIDE >



PHYSICAL SECURITY.

Physical security.

A **mantrap**, now referred to as an **access control vestibule**, is found at the entrance to secure sections of the building and involves two doors, one right after the other. The first door may or may not require authentication to enter; it is close enough to the other door to permit only one person between them at a time, and the first door must be closed behind you before you can attempt to open the second. If you cannot authenticate to the second, the first door cannot be opened from the inside, so you are trapped until the building security comes to get you.



PHYSICAL SECURITY.

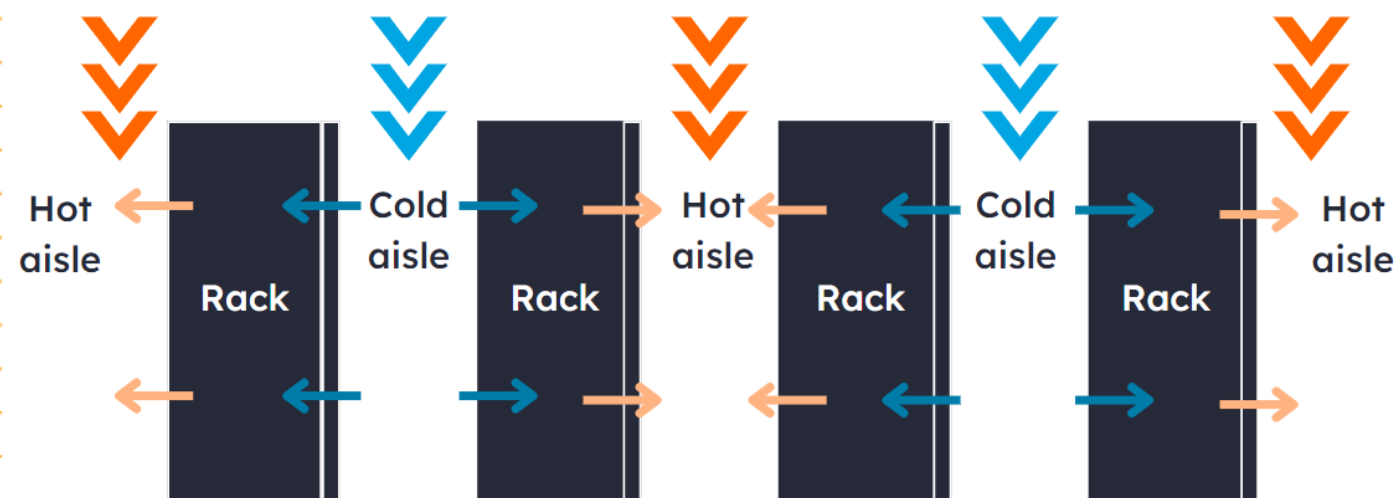
Facility security.



- Bollards/barricades
- Badges
- Signage
- Lighting
- Fencing

PHYSICAL SECURITY.

Secure areas.



A **vault** is a secure room hardened against entry by unauthorized individuals.

Safes can protect data in several formats against unauthorized disclosure. Many are also fire and water-resistant.

Hot and cold aisles – In server rooms, racks of servers are configured so that the backs of the servers in a rack face the backs of the next rack of servers; this creates a hot aisle as the hot air exits the backs of the servers. Conversely, the fronts of servers will face each other, creating a cold aisle. The HVAC airflow then removes the hot air from the hot aisle exhausting it outside the facility. The cold air is forced through the servers from the cold aisle.

CONTINUED ON NEXT SLIDE >

PHYSICAL SECURITY.

Secure areas.



- **Colocation** involves a facility hosting several companies, in which those companies share caged space to secure their servers together.

- Due to the nature of some computing devices, a security zone technique known as an “**air gap**” may physically isolate a network or single device from others. No communication is allowed through the “air gap.”

PHYSICAL SECURITY.

Video surveillance and security personnel.

Video surveillance broadens the area that can be secured by minimally staffed security. Cameras are used both as a preventative and detective control.



CONTINUED ON NEXT SLIDE >

PHYSICAL SECURITY.

Video surveillance and security personnel.



PHYSICAL SECURITY.

Locks.



Electronic

Biometrics

Physical

Cable locks

USB data blocker

PHYSICAL SECURITY.

Sensors and alarms.

- Motion detection
- Noise detection
- Proximity reader
- Moisture detection
- Cards
- Temperature
- Circuit
- Duress alarms

PHYSICAL SECURITY.

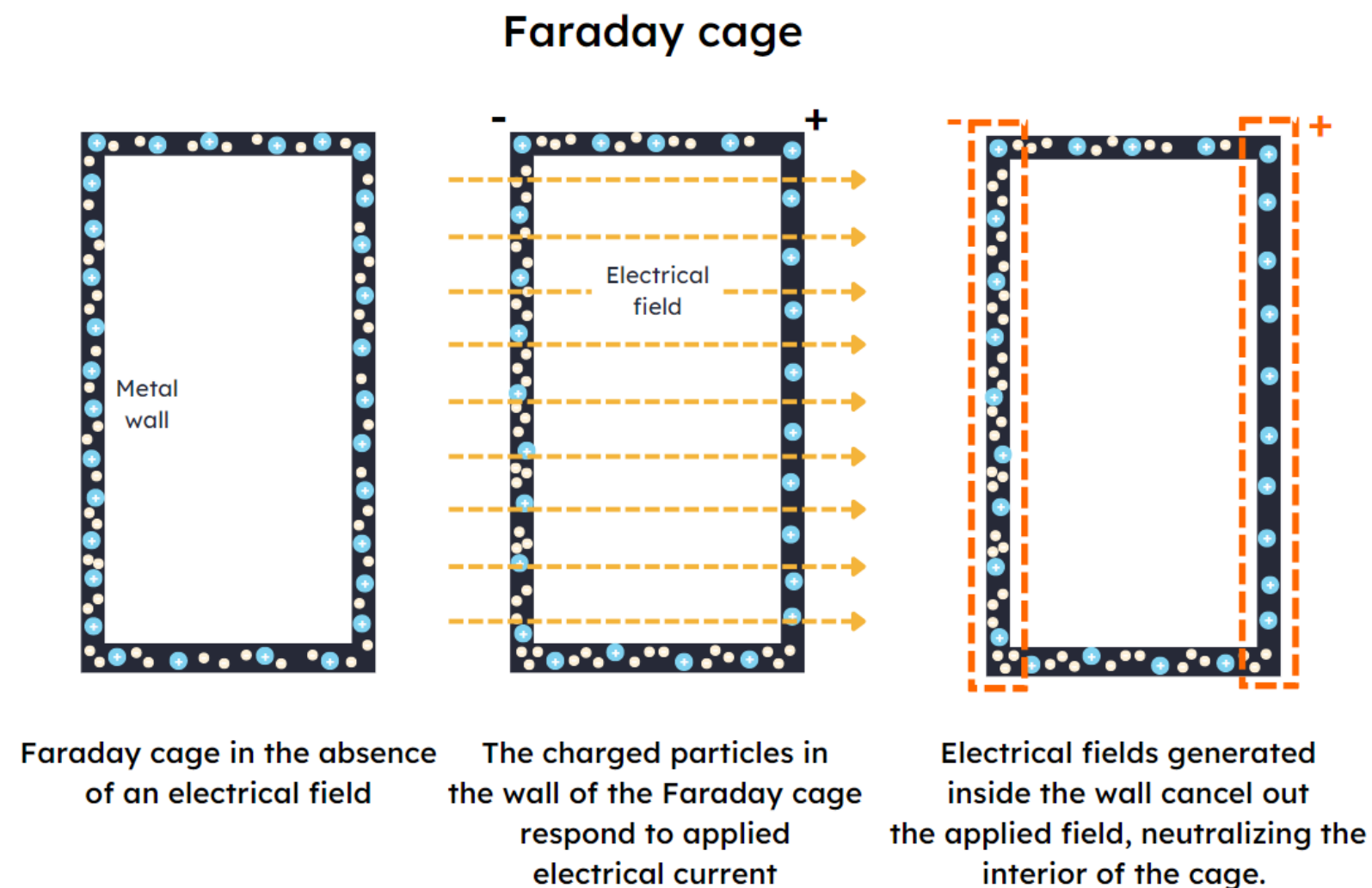
Secure data destruction.

- Secure data destruction
- Degaussing
- Data wiping and overwriting
- Burning Shredding
- Pulping
- Pulverizing



PHYSICAL SECURITY.

Physical data security.








Protecting physical access to Wi-Fi might include a **Faraday cage** or **Faraday wallpaper**, capable of blocking a radio signal from escaping outside the confines of the building.

Protected cable distribution is used to secure physical access to wired networks by fully enclosing the cable trays that support horizontal cabling.

Fire suppression.

Fire suppression systems are in place as a safety measure for personnel; they are also there to preserve data and systems from being destroyed due to a fire.

A		Common Combustibles	Wood, paper, cloth etc.
B		Flammable liquids and gases	Gasoline, propane and solvents
C		Live electrical equipment	Computers, fax machines
D		Combustible metals	Magnesium, lithium, titanium
K		Cooking media	Cooking oils and fats



PHYSICAL SECURITY.

Fire suppression.

Sprinkler systems can be of the following types:

- Wet-pipe
- Dry-pipe
- Pre-action
- Halon Clean Agent

PHYSICAL SECURITY.

Knowledge Check.

Let's apply what we have covered:

- Discuss the various forms of secure data destruction.
- Discuss the various forms of sensors and alarms.



Access Controls.



ACCESS CONTROLS.

Access Controls.

In this section, we will cover the following key concepts:

- Access Control Lists.
- Access Control Models.
- Discretionary Access Control.
- Mandatory Access Control.
- Rule- and Role-Based Access Control.
- Attribute-Based Access Control.



ACCESS CONTROLS.

Access Control Lists (ACLs).



- Access control lists (ACLs) are a list of rules that apply permissions and grant authorization based on authentication. ACLs may be enforced by a firewall.

- It is not very common knowledge that the permission set on an NTFS file is a form of ACL; this is due to the permissions being a means of controlling who is allowed to access which portions of data in that file or folder.

ACCESS CONTROLS.

Access control models.



- The three **access control** models are DAC, MAC, and RBAC; these three variations in access control can provide a great deal of security to a network.
- Each access control model serves a different purpose.
- You will most likely implement some variation of access control in your future position. Most organizations (due to the nature of today's risk) utilize various AC models to accomplish data and privacy protection.

ACCESS CONTROLS.

Discretionary Access Control (DAC).



- Discretionary access control (DAC) is the most common method of access control based on authorization on an item, such as a folder and its permissions in NTFS. It is also the default method of access control for both Windows and Linux.

- Setting up directories and folders on a Linux machine will require students to know how file permissions work.

- Linux machines utilize three different 3-bit sets of letters to identify permissions across the device (or network): read, write, and execute. These three sets of letters are defined by three entities: the owner, the group, and the world. These separations in permissions are considered DAC.

ACCESS CONTROLS.

Mandatory Access Control (MAC).



- Mandatory access control (MAC) is an access control model based on a label assigned to a resource. Labels represent security clearance levels and may include “confidential”, “secret”, and “top-secret”, even within non-military organizations.

MAC methods are generally implemented in the form of permissions assigned to a device, which prevents a user from escalating privileges or taking control of the machine.

ACCESS CONTROLS.

Role-based and rule-based access control.



- **Role-based access control (RBAC)** bases your access on your job title. Many web-based environments assign permissions based on roles.

- **Rule-based access control** bases your access to a system or resource depending on system rules rather than system users.

ACCESS CONTROLS.

Attribute-Based Access Control (ABAC).



Attribute-based access control (ABAC) is a method of restricting resource access based on a series of determining factors, such as the user's name, time of day, or location.

ACCESS CONTROLS.

Knowledge Check.

Let's apply what we have covered:

- Describe mandatory access control.
- How is discretionary access control implemented?



Privacy and Sensitive Data Security.



PRIVACY AND SENSITIVE DATA SECURITY.

Privacy and Sensitive Data Security.

In this section, we will cover the following key concepts:

- Information Lifecycle.
- Terms of Agreement.
- Technologies.
- Data Types.
- Data Classifications.
- Roles and Responsibilities.
- Data Protection.
- Data Loss Prevention.
- Geographic Considerations.



PRIVACY AND SENSITIVE DATA SECURITY.

Information lifecycle.

Data is the most important asset most organizations have — it is at the center of the CIA Triad, and most security policies are designed to protect it in one way or another. Data (information) itself has a lifecycle; stages of the information lifecycle are:

- Creation/Collection
- Distribution/Use
- Retention
- Disposal

As a part of Information Lifecycle Management, a process known as an **impact assessment** is done; it is designed to identify the risks of data throughout its lifecycle. An assessment also reviews business workflows using data and how to mitigate risks.

PRIVACY AND SENSITIVE DATA SECURITY.

Privacy terms of agreement.

Organizations are ultimately responsible for the security of their data, even though they often outsource many services to a third party. Issues around the security of data sets are formalized in legal agreements:



Service-Level Agreement (SLA)

Interconnection Security Agreement (ISA)

Nondisclosure Agreement (NDA)

Data Sharing and Use Agreements

Privacy enhancing technologies.

Data minimization is the principle of sufficiency or adequacy in data collection means that you should only collect data specifically stated for the purpose of a transaction, and the user must give consent to that data collection.

Data masking – An irreversible method that redacts data by substituting “X” or “*” in the character strings, for example.

Tokenization – A reversible method that replaces all or part of a field of data with a random token; this can be used as a substitution for encryption.

Aggregation/Banding – This method is used to generalize data — for instance, by replacing specific ages with aged bands: 50-59 years.

Data types.

Data types are a schema that identifies a category of data that can be regulated by governments or have best practices identified by standards organizations. Some important data types are:

- Personally Identifiable Information (PII)
- Personal Health Information (PHI)
- Financial Information
- Government Data
- Customer Data

Data classifications/labels.

Security labels (or classifications) are used to identify the sensitivity classification of the data and documentation and are categorized based on who can access the data, document, or object:

- **Public (unclassified)** – No restrictions on viewing the data. The data presents no risk to the organization.
- **Private** – Information about a specific individual identity.
- **Sensitive** – Generally used in the context of personal data.
- **Confidential (secret)** – Highly-sensitive information that is viewable to approved personnel or individuals who have signed an NDA.
- **Critical (top secret)** – Information too valuable to be released to anyone outside the organization.
- **Proprietary (intellectual property)** – Information created and owned by the organization. IP is often targeted by competitors.

PRIVACY AND SENSITIVE DATA SECURITY.

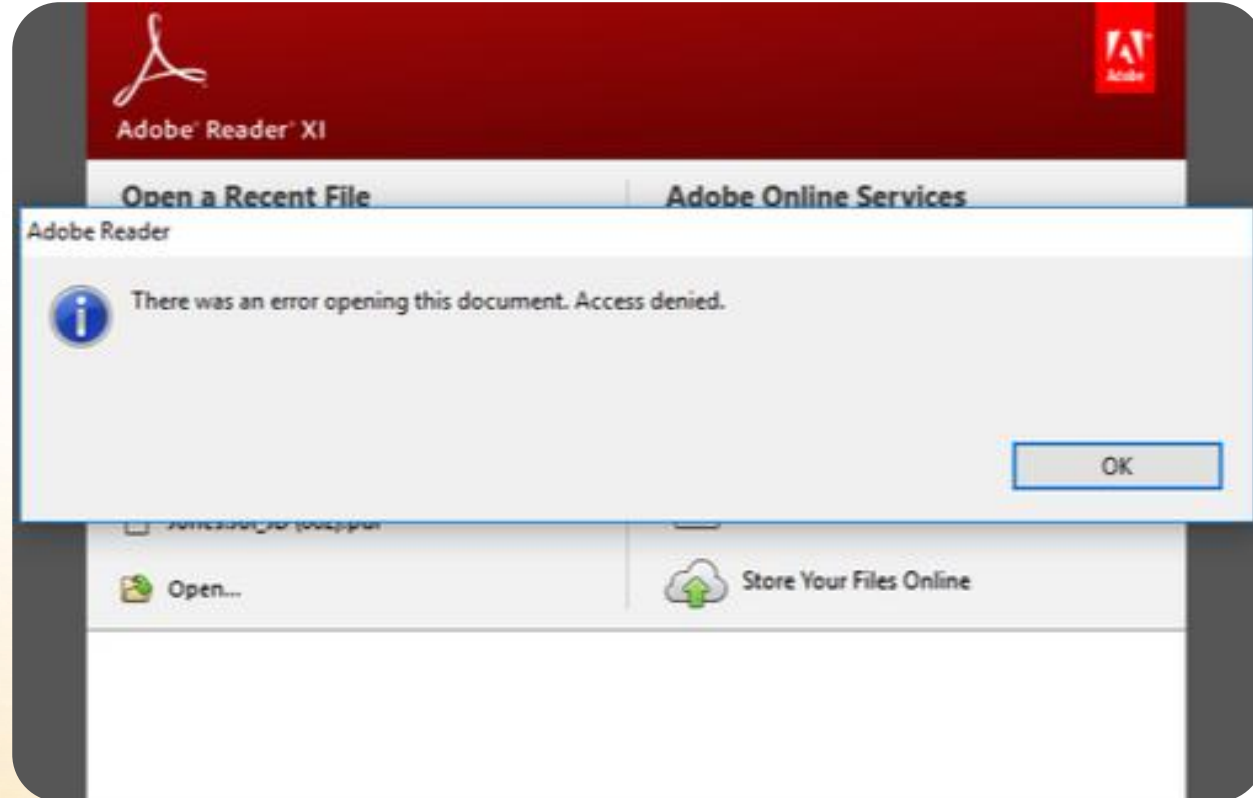
Roles and responsibilities.

- Data Owner
- Data Steward
- Data Custodians
- Data Protection Officers (DPOs)
- Data Controllers
- Data Processors



PRIVACY AND SENSITIVE DATA SECURITY.

Data protection.



Data at rest

Data in transit/motion

Data in use

Information Rights Management

Data loss protection.

Data loss prevention (DLP) is another technology that works to keep classified/labeled information from unauthorized exfiltration. Solutions have different parts:

● **Policy server** – Configures the classification rules and policies required for enforcement.

● **Endpoint agents** – Enforce policy on endpoints.

● **Network agents** – Scan communications on the network for policy violations.

CONTINUED ON NEXT SLIDE >

Data loss protection.

Should a policy violation occur, a document can be placed into one of several remediation options:

Alert only – Administrators are only notified of the violation. The transaction is permitted to occur.

Block – Copying or sending is prohibited; a log entry is made, and notifications are sent.

Quarantine – The original document is no longer available to the offending user, and the transaction is blocked.

Tombstone – Quarantine with the addition of a replacement file describing the violation and how to release the original document within policy guidelines.

Geographic considerations.

Security professionals must now consider geographical issues when considering how best to secure data.

Data sovereignty – This means a jurisdiction can place a restriction on the ability of an organization to process or store data on systems that are not physically located within that jurisdiction; the impact of this may cause companies to move data to a different geographic location where the laws of jurisdiction are more favorable.

PRIVACY AND SENSITIVE DATA SECURITY.

Knowledge Check.

Let's apply what we have covered:

- What are the differences between a data custodian, data steward, and data processor?
- What are some geographic considerations concerning data security?





End of Module.

Part – 1

For additional practice, please complete all associated self-study activities and labs.