Domain 3: Access Control Concepts

▼ Security Control Protocols

Concepts Covered:

- Security Controls
- Controls Overview
- Examples of Least Privilege
- Separation of Duties
- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Mandatory Access Control (MAC) in the Workplace

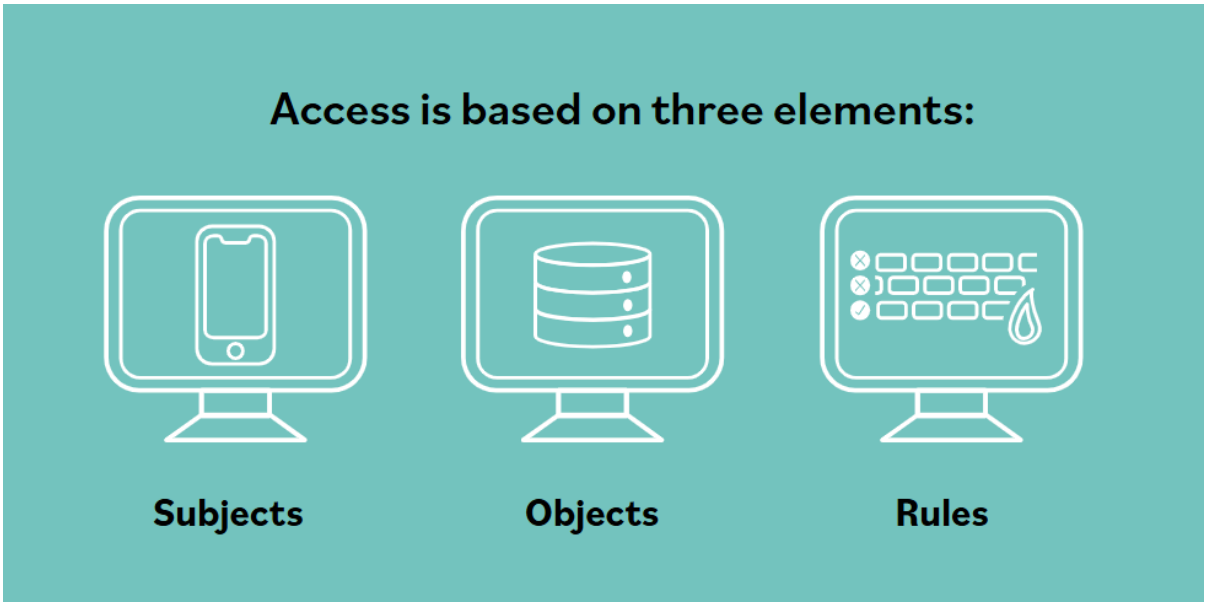
1. Security Controls Overview

- **Definition:** Security controls are safeguards or countermeasures designed to preserve the Confidentiality, Integrity, and Availability (CIA Triad) of data.
- **Example:** A firewall acts as a control by blocking unauthorized access from outside and preventing sensitive internal information from leaking out.

2. Access Control

- **Purpose:** Determines which subjects (users, processes, etc.) can access which objects (files, devices, etc.) and under what conditions.
- **Importance:** Central to information security; controls both restriction and granting of access.

3. Key Concepts



Subject

- **Definition:** Any entity that requests access to resources (active initiator).
- **Examples:** User, process, client, server, device (e.g., smartphone, USB drive).
- **Characteristics:**
  - Initiates requests for services.
  - Must have appropriate permissions (clearance).

Object

- **Definition:** Anything a subject attempts to access (passive responder).
- **Examples:** File, database, printer, server, memory block, building.
- **Characteristics:**
  - Responds to access requests.
  - Does not contain its own access control logic.
  - Access rules are managed externally (e.g., access control lists).

Rule

- **Definition:** Instruction that allows or denies access to objects based on subject's validated identity and permissions.
- **Examples:**
  - Firewall rule allowing internal network access to the internet.
  - File access rule permitting a user to read but not modify a document.
- **Capabilities:**
  - Can compare multiple attributes.
  - Allow, deny, or limit access (e.g., time-based restrictions).

4. Principle of Least Privilege

- **Definition:** Users are granted only the minimum access necessary to perform their job.
- **Examples:**
  - Only billing staff can view financial data; only a few can modify it.
  - Healthcare workers may access patient contact info but not medical records unless necessary.
- **Features:**
  - Temporary or limited access (e.g., only during business hours).
  - Monitoring and alerts for unauthorized access attempts.
  - Critical access often requires multi-factor authentication.

5. Separation of Duties

- **Definition:** No single person should control all parts of a high-risk transaction.
- **Implementation:**
  - Tasks are divided among multiple people (e.g., one submits an invoice, another approves it).
  - Prevents fraud and errors.

    - **Collusion:** Two or more people working together to bypass controls.
- **Dual Control Example:** Bank vault with two combination locks, each known by a different person.
- **Two-Person Integrity:** Requires at least two people present in high-security areas to prevent unauthorized actions and ensure safety.

6. Access Control Models

Discretionary Access Control (DAC)

- **Definition:** Access rights are at the discretion of the object owner.
- **Capabilities:**
    - Owners can grant, revoke, or transfer access.
    - Users can share files or resources as they see fit.
- **Examples:**
    - In Unix/Windows, file owners set permissions for others.
    - Sharing a file on Google Drive and choosing who can view or edit it.
    - Visitor badges issued at a security desk.
- **Limitations:** Not very scalable; difficult to track access issues.

Mandatory Access Control (MAC)

- **Definition:** Access rights are centrally controlled by security administrators, not by individual owners.
- **Enforcement:** Uniformly applied across all subjects and objects; only admins can change permissions.
- **Examples:**
    - Government agencies require security clearances for access to sensitive areas.
    - Access determined by policy, not individual discretion.

- **Features:**
  - Subjects cannot pass on privileges or change rules.
  - Often combined with separation of duties and role-based access control.

7. Summary Table

Concept	Who Controls Access?	Example
DAC	Object owner (user)	File sharing permissions in Windows/Unix
MAC	Security admin/policy	Security clearance in government agencies
Least Privilege	Admins (by role/job)	Billing staff access to financial data
Separation of Duties	Process design	Invoice submission and approval by different people
Two-Person Integrity	Physical security	Two people required to open a bank vault

8. Key Takeaways

- Security controls protect data’s confidentiality, integrity, and availability.
- Access controls define who can access what, and how.
- Least privilege and separation of duties are critical for minimizing risk.
- DAC is flexible but less secure; MAC is rigid but more secure.
- Real-world examples include firewalls, file permissions, security clearances, and dual-control vaults.

▼ Access Control Strategies

Concepts Covered:

- Controls Assessments

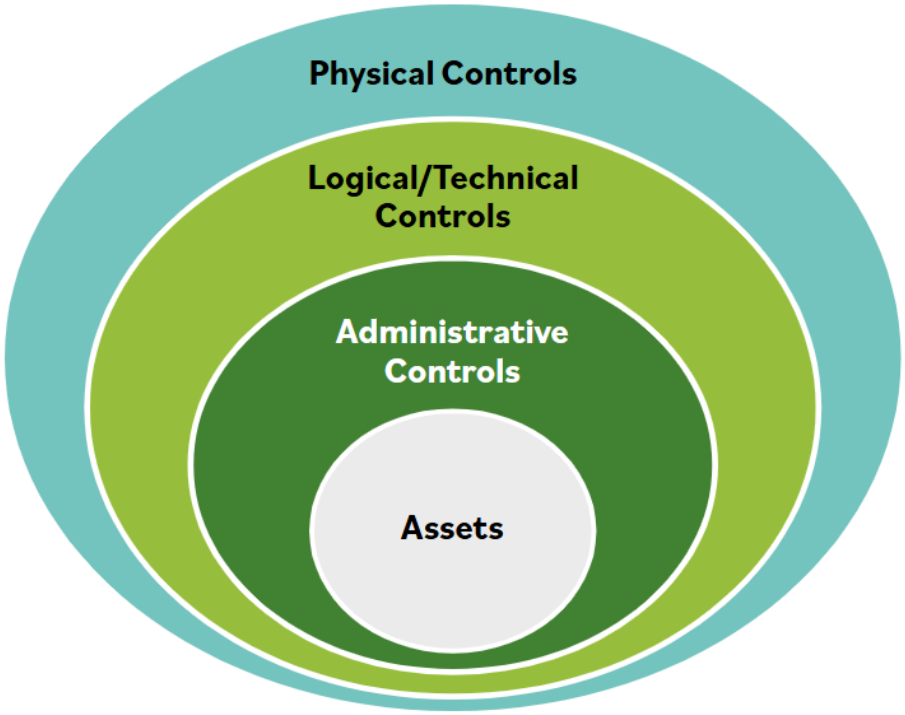
- Defense in Depth
- Defense in Depth in Practice
- The Benefit of Multiple Controls
- Physical Security Controls
- Types of Physical Access Controls
- Monitoring
- Logical Access Controls

Controls Assessments

- **Effectiveness of Controls**
  - Risk reduction relies on how effective controls are.
  - Controls must be relevant to the current situation and adaptable to changes.
- **Scenario Example: Securing a Repurposed Office Area**
  - Office area being converted to a secure storage facility.
  - Five doors need securing before storing confidential files.
  - Considerations:
    - Install biometric scanners on all or some doors based on a site assessment.
    - Alternative: Permanently secure or remove some doors, replacing them with walls if budget allows.
    - Cost of controls should match the value of the protected asset.
- **Control Selection**
  - If full biometric security is unnecessary, simpler solutions like deadbolt locks may suffice.
  - The level of control should be appropriate for the security need.

Defense in Depth

- **Definition**
  - A layered security strategy integrating people, technology, and operations.
  - Applies multiple countermeasures at different levels.
- **Purpose**
  - To prevent or deter cyberattacks.
  - No guarantee of complete prevention.
- **Technical Example: Multi-Factor Authentication**
  - Username + password (something you know) + code sent to phone (something you have).
  - More secure than either method alone.
- **Technical Example: Multiple Firewalls**
  - Separate untrusted (e.g., internet) and trusted networks.
  - Sensitive data stored behind multiple firewalls.
- **Non-Technical Example: Data Center Access**
  - Physical lock on the door (physical barrier).
  - Technical access rules (e.g., network restrictions).
  - Administrative policies (define who is authorized).



Defense in Depth in Practice

- **Multiple Layers of Defense**
  - Administrative controls: Policies and procedures.
  - Technical controls: Programming, logical access restrictions.
  - Physical controls: Physical barriers and security measures.
  - Even with cloud services, physical storage and processing still exist.

The Benefit of Multiple Controls

- **Definition of a Control**
  - Safeguard or countermeasure for confidentiality, integrity, and availability.
- **Example: Payroll System**

    - Risk: Payroll personnel could create fake employees and process fraudulent checks.
    - Controls:
        - Technical: Prevent same person from creating and processing payroll records.
        - Physical: Secure check printing media so payroll processor cannot access it.
        - Administrative: Policies for regular audits and verification of new employees and check numbers.
    - Small businesses may rely more on physical and logical controls due to limited staff.

Physical Security Controls

What are Physical Security Controls?

- **Definition**
    - Tangible items/mechanisms to prevent, monitor, or detect physical access.
- **Examples**
    - Security guards, fences, motion detectors, locked doors/gates, sealed windows, lighting, cable protection, laptop locks, badges, swipe cards, guard dogs, cameras, mantraps/turnstiles, alarms.
- **Purpose**
    - Protect company assets, especially personnel.

Why Have Physical Security Controls?

- **Purpose**
    - Prevent unauthorized physical entry.
    - Protect both assets and personnel safety.

Types of Physical Access Controls

Badge Systems and Gate Entry

- **Technologies**
  - Turnstiles, mantraps, system-controlled doors.
  - Enrollment stations assign badges with access permissions.
  - High-security: May include biometrics.
  - System checks badge against database, logs access events.
- **Card Types**
  - Bar code, magnetic stripe, proximity, smart, hybrid cards.

Environmental Design (CPTED)

- **Approach**
  - Uses passive design elements to deter crime.
  - Involves organizational (people), mechanical (technology), and natural (architecture/flow) methods.
  - Example: Designing spaces for visibility to reduce hidden areas.

Biometrics

- **Definition**
  - Authentication using unique individual characteristics.
- **Processes**
  - Enrollment: Store biometric code in system or on a smart card.
  - Verification: Compare presented data to stored code.
- **Types**
  - Physiological: Fingerprints, iris, retina, palm, venous scans.
  - Behavioral: Voiceprints, signature dynamics, keystroke dynamics.

- **Considerations**
  - Highly accurate but costly.
  - Privacy concerns and device sanitization issues.

Monitoring

- **Purpose**
  - Track personnel/equipment entry and exit.
  - Audit and log all physical events.

Monitoring Examples

- **Cameras**
  - Central monitoring, deterrence, detection, and forensic evidence.
  - Used in hard-to-access or sensitive areas.
- **Motion Sensors**
  - Infrared, microwave, laser, vibration sensors for perimeter security.
- **Logs**
  - Records of access events (manual or electronic).
  - Must be protected, reviewed regularly, and retained per legal/business requirements.
  - Example: PCI DSS requires one year of log retention.
  - Anomalies in logs can indicate security issues.
- **Alarm Systems**
  - Alert personnel to unauthorized access or emergencies (fire, panic buttons).
  - Example: Door alarms trigger if opened without authorization.
- **Security Guards**
  - Provide deterrence and monitoring.

    - Prevent unauthorized access and tailgating.

Logical Access Controls

- **Definition**
    - Electronic methods to restrict access to systems or assets.
- **Examples**
    - Passwords, system-implemented biometrics, badge/token readers.
- **Purpose**
    - Restrict logical access, even if physical access is possible.

Summary:

Effective security requires a combination of physical, logical, and administrative controls, often implemented in layers (defense in depth). Each control should be appropriate to the value and risk of the asset being protected. Examples range from simple locks and policies to advanced biometrics and multi-factor authentication, with monitoring and logging playing a critical role in detection and response.

▼ User Privilege Administration

Concepts Covered:

- Privileged Access Management
- Privileged Accounts
- Authorized Versus Unauthorized Personnel
- Role-Based Access Control
- Role-Based Access Control (RBAC) in the Workplace

Privileged Access Management (PAM)

- **Definition:** Controls and manages elevated access and permissions for users (e.g., admins) to critical systems and data.
- **Traditional Approach:** Privileges assigned statically to admin users, active 24/7; security relies mainly on login credentials.
- **Just-in-Time PAM:** Privileges are granted dynamically, only when needed, and for specific tasks.
    - **Example:** An admin receives elevated access to a database only during maintenance windows, not all the time.
- **Importance:**
    - Prevents misuse of always-on admin accounts.
    - Reduces risk if credentials are compromised.
- **Case Example:**
    - **Scenario:** ABC, Inc. IT staff added themselves to "Domain Admins" for convenience.
    - **Incident:** Opened a ransomware email while logged in as Domain Admin; ransomware encrypted all files across the network.
    - **PAM Solution:** If admin privileges were only enabled for specific tasks, the attack's impact would be limited.

Privileged Accounts

- **Definition:** Accounts with higher permissions than standard users (e.g., managers, admins).
- **Types of Privileged Users:**
    - **System Administrators:** Manage OS, applications, and performance.
    - **Help Desk/IT Support:** Reset passwords, unlock accounts, manipulate endpoints.
    - **Security Analysts:** Need broad access for incident response.
    - **Project/Client Accounts:** Temporary elevated access for specific needs.

- **Delegation:** Access should be assigned based on trust and necessity.
- **Risk Mitigation Measures:**
  - **Detailed Logging:** All privileged actions are logged for deterrence and audit.
    - *Example:* Logging every password reset by Help Desk staff.
  - **Stringent Access Control:** Use of Multi-Factor Authentication (MFA) and just-in-time privileges.
  - **Trust Verification:** Background checks, NDAs, and ongoing vetting.
  - **Frequent Auditing:** Privileged accounts are audited more than regular accounts.
- **Help Desk Example:**
  - Only grant "reset password" and "unlock account" permissions, not full admin rights.
  - Actions are logged and matched with support tickets for verification.

Authorized vs. Unauthorized Personnel

- **Process:**
  - **Authentication:** Verifying user identity (e.g., badge, password).
  - **Authorization:** Checking if authenticated user has permission for the action.
    - *Example 1:* Data center door unlocks only for authorized badge IDs.
    - *Example 2:* File deletion allowed only if user has delete permission.

User Provisioning

- **New Employee:** Manager requests account creation with defined access.
- **Change of Position:** Update access rights as per new role; remove unneeded permissions.

- **Separation:** Disable account upon exit; keep disabled for audit before deletion.
- **Best Practice:** Do not copy old user profiles to new users to prevent privilege creep.
    - *Example:* If a user temporarily got extra access, copying their profile to a new hire spreads unnecessary permissions.

Role-Based Access Control (RBAC)

- **Definition:** Access rights are grouped by role; users are assigned roles based on their job.
- **Process:**
    - Assign users to roles (e.g., HR, Finance, Manager).
    - Grant/revoke access by changing role assignments.
- **Benefits:** Efficient for organizations with high staff turnover and similar access needs.
- **Example:** Only HR can access personnel files; only Finance can access bank accounts.
- **Risk:** Privilege creep if roles are not regularly reviewed.
- **Best Practice:** Use standard roles for new users, not copied profiles.

Comparison Table: Access Control Models

Model	Definition	Example
DAC (Discretionary Access Control)	Resource owners decide who has access to their resources.	File owner sets permissions for who can read/write their files.
MAC (Mandatory Access Control)	Access decisions are based on fixed policies set by the system, not by users.	Military classification: Only users with "Top Secret" clearance can access certain files.

Model	Definition	Example
RBAC (Role-Based Access Control)	Access is based on roles assigned to users, not individual permissions.	HR staff can access employee records; Finance can access payroll data.
RuBAC (Rule-Based Access Control)	Access is determined by system-enforced rules (often used with RBAC).	Only allow access to payroll systems during business hours.
ABAC (Attribute-Based Access Control)	Access is based on user, resource, and environmental attributes.	Only users in the "Manager" group, in the "Sales" department, and in the office can access a report.
PBAC (Policy-Based Access Control)	Access is governed by policies that combine rules, roles, and attributes.	Allow access to sensitive data only if user is in compliance with training requirements.

Summary Table

Model	Who Controls Access?	Based On	Example
DAC	Resource Owner	User discretion	File sharing in Windows: owner grants access
MAC	System/Policy	Security labels	Classified military documents
RBAC	Admin/Organization	User roles	HR can access employee records
RuBAC	System/Policy	Rules (conditions)	Access only during work hours
ABAC	System/Policy	Attributes (user, resource, context)	Only managers in Sales can access Q2 report
PBAC	System/Policy	Policies (combining roles, rules, attributes)	Access if compliance training completed

In summary:

- Privileged access management is critical to limit risks from elevated permissions.
- Access controls (DAC, MAC, RBAC, RuBAC, ABAC, PBAC) differ in how and who determines access, and each has its own best-use scenarios and examples.
- Regular review, logging, and least privilege principles are essential for robust security.