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

Definition:

Security controls are safeguards or countermeasures designed to protect the **Confidentiality, Integrity, and Availability (CIA Triad)** of data and systems.

Purpose:

- Prevent unauthorized access or damage to data/information systems.
- Ensure only authorized subjects access specific objects under defined rules.

Example:

- **Firewall:**

  Acts as a barrier between an internal network and external networks (like the Internet).

  - Prevents unauthorized external access to internal network resources.
  - Restricts unauthorized outbound traffic to protect sensitive information inside the network.

2. Controls Overview

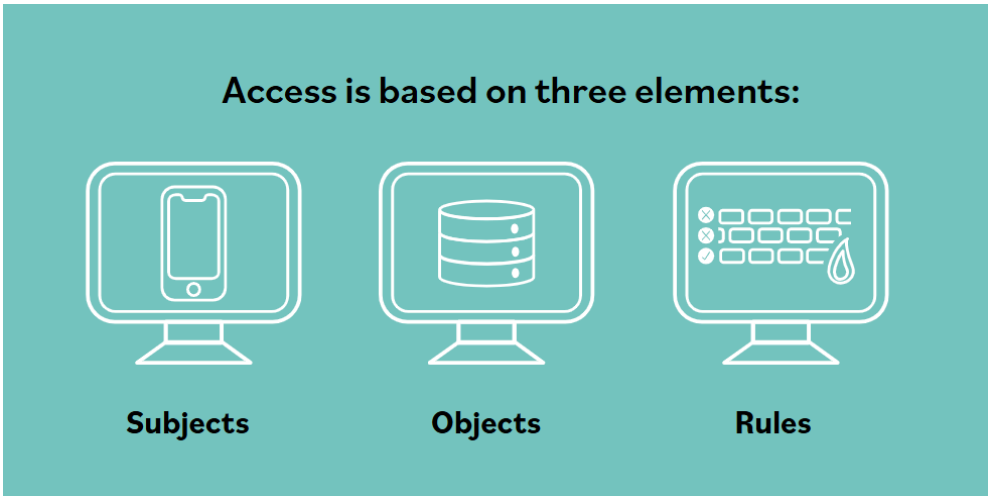
Core Idea:

- **Access Control** is the centerpiece of information security programs. It manages **who** can access **what** assets and **what actions** they can perform.

Access Control Includes:

- Both **granting** and **restricting** access appropriately to authorized and unauthorized entities.

Key Terms:



Subject:

- An **active entity** requesting access to assets.
- Can be a user, client, process, program, device, etc.
- Initiates access requests to objects.
- Must have permissions or clearance to access resources.

Examples:

- Employee logging into a database.
- A software process attempting to read a file.

Object:

- A **passive entity** being accessed or requested by a subject.
- Can be any resource such as files, databases, servers, printers, memory blocks, or even persons/services.
- Objects don't enforce access control themselves; protection is provided by external mechanisms like identity and access management systems.
- Have owners who define access permissions, often recorded in access control lists or rule bases.

Examples:

- A patient database file.
- A network printer.

Rule:

- A formal instruction determining whether a subject may or may not access an object.
- Rules reference attributes and permissions, and can:
  - Allow or deny access.
  - Define how much or what kind of access is allowed.
  - Apply time-based or conditional access.

Example:

- Firewall rule permitting outbound traffic from internal network IPs to web servers.

3. Examples of Least Privilege

Principle of Least Privilege:

- Grant users the **minimum access rights** needed to perform their job functions — nothing more.

Examples:

- Billing staff can view financial data but not modify it.
- Doctors access only their patients' medical records, according to HIPAA regulations.
- Temporary access provided during a limited time window or business hours.

Additional Security:

- Access monitoring and logging alert administrators to unauthorized attempts.
- Higher sensitivity requires stronger safeguards (e.g., multi-factor authentication).

4. Separation of Duties (SoD)

Concept:

- No single individual should control an entire critical process end to end.
- Splits high-risk tasks into multiple parts, delegated to different people to prevent errors or fraud.

Examples:

- Invoice submission by an employee, approval by a manager.
- System change requests reviewed and approved by different departments.

Related Concepts:

Collusion:

- When two or more individuals collaborate to bypass separation of duties, committing fraud.

Dual Control:

- Requires two individuals to perform a task together for added security (e.g., two-lock combinations to open a vault).

Two-Person Integrity:

- Security policy requiring at least two individuals present in sensitive areas.
- Mitigates insider threats and provides life safety support.

5. Discretionary Access Control (DAC)

Overview:

- Access control policy where the **owner of the resource** decides who can access it and what privileges they have.

- Subject (user) with access to an object may pass that access or change permissions.

Characteristics:

- Flexible but can become difficult to manage & audit at scale.
- Access control lists (ACLs) and capability lists map subjects to objects and permissions.

Example:

- In UNIX/Linux, file owners set permissions on files they create.
- Windows file sharing permissions set by the file creator or administrator.
- Temporary visitor badges granted at a security desk.

6. Mandatory Access Control (MAC)

Overview:

- Access control policy enforced **uniformly** by the system.
- Only **security administrators** can modify access rules.
- Subjects are constrained and cannot modify permissions or share information arbitrarily.
- Access decisions depend on classification labels and security clearances.

Key Differences from DAC:

- Access rights are assigned by trusted administrators, **not** by individual owners.
- Subjects cannot delegate or alter permissions.

7. Mandatory Access Control (MAC) in the Workplace

Implementation:

- Access restrictions enforced by organization-wide policies—little or no individual discretion.
- Security clearances required for access (e.g., classified government information).
- Enforced Separation of Duties and Role-Based Access Control typically complement MAC.

Example:

- Government agencies where users must have specific clearance levels to enter secure zones.
- Employees have access limited strictly to information related to their role or duties.

Summary Table of Access Control Key Concepts

Concept	Subject (Active)	Object (Passive)	Key Policy Points	Control Authority
Access Control	Entity requesting access	Entity being accessed	Who, what, when, how	Varies
Least Privilege	Users have minimal necessary access	Data and resources limited appropriately	Restrict access tightly to need	Owner/Administrator
Separation of Duties	Different people for different transaction parts	Resources involved in processes	Prevent fraud via role separation	Organizational Policies

Concept	Subject (Active)	Object (Passive)	Key Policy Points	Control Authority
DAC	Users can pass on their own access permissions	Resource owners control their own objects	Owner discretion, flexible but less scalable	Resource Owners
MAC	Subjects must have assigned clearances	Objects labeled with security classification	Enforced by admins, non-discretionary	Security Administrators

▼ 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

1. Controls Assessments

Definition:

Controls assessments evaluate how effectively security controls reduce risk in a given environment. The control must be suitable for the current situation and adaptable to changes.

Key Points:

- Controls must match the environment and evolving threats.
- Implementation cost of controls should be proportional to the value of assets protected.
- Example Scenario:
  - An office area is converted into a secure storage room with 5 existing doors.
  - Assessment might recommend biometric scanners on all doors, or fewer, depending on risk.
  - Alternative controls include permanently securing or removing doors if budget permits.
  - If high auditing or strict logging isn't essential, simpler controls (e.g., deadbolt locks) might suffice.

Summary:

A site assessment helps decide which controls are necessary, balancing security effectiveness and cost.

2. Defense in Depth

Definition:

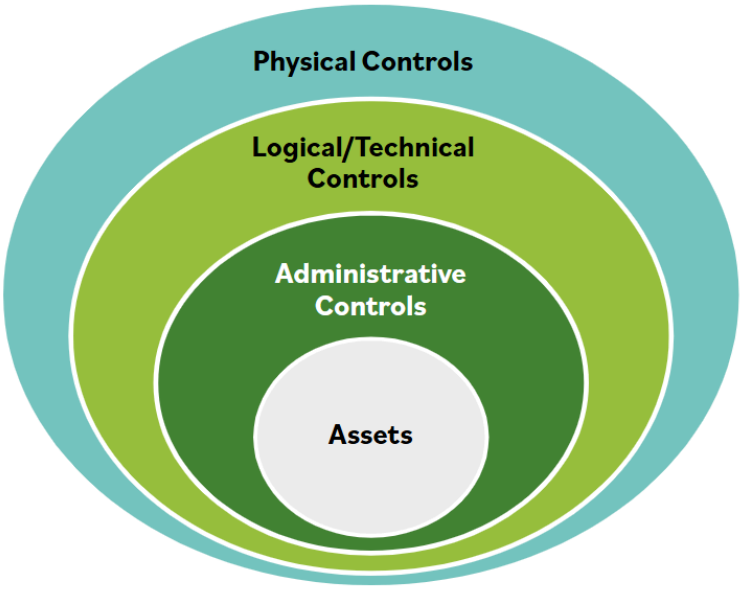
Defense in depth is a layered security strategy integrating people, technology, and operational processes to establish multiple barriers protecting information assets.

Key Points:

- Applies multiple countermeasures across different layers.
- It is a preventive strategy but does *not* guarantee absolute security.
- Includes all forms of access control: physical, logical, administrative.

Examples:

- **Technical Layered Control:**
  - Login requires username/password (something you know) + code on phone (something you have) = Multi-Factor Authentication (MFA).
- **Network Layer:**
  - Multiple firewalls segregate internet, trusted networks, and critical data centers.
- **Non-Technical Layer:**
  - Physical locks securing data centers.
  - Access control policies defining authorized personnel.



3. Defense in Depth in Practice

Context:

Even in modern environments like cloud computing, physical controls and locations are essential.

Key Points:

- Beyond cloud's virtual nature, data still resides on physical hardware in data centers.
- Security involves administrative controls (policies), logical controls (software access restrictions), and physical controls (locked rooms, secured hardware).
- All layers must function together for effective security.

4. The Benefit of Multiple Controls

Definition:

A control is any safeguard aimed at preserving confidentiality, integrity, and availability (CIA) of data.

Use Case – Payroll System:

- Payroll is a common high-risk area requiring multiple controls.
- **Technical Control:** Restrict payroll processors from creating new employee records.
- **Physical Control:** Secure physical access to check-printing paper/media.
- **Administrative Control:** Regular audits and reviews of employee records and printed checks.

Challenges:

- Small/medium businesses often lack sufficient staff for separation of duties.
- They may rely more on physical and administrative controls rather than technical controls due to resource constraints.

5. Physical Security Controls

Definition:

Controls that physically prevent or detect unauthorized access to assets or personnel.

Examples:

- Security guards, fences, locked doors, biometric scanners, surveillance cameras, motion detectors, badges, swipe cards, alarms, mantraps/turnstiles, cable locks.

Purpose:

- Protect people's safety first, then physical assets.
- Prevent unauthorized entry into secure areas.

6. Types of Physical Access Controls

Badge Systems and Gate Entry

- Use badges, cards, or biometrics combined with technology like turnstiles and door locks.
- Enrollment station issues badges with access permissions.
- Card types include: Bar code, magnetic stripe, proximity, smart, and hybrid cards.

Environmental Design (CPTED)

- Incorporates architectural design to prevent crime—natural surveillance, clear flow control, and robust visibility.
- Uses organizational, mechanical, and natural design elements to discourage unauthorized access.

Biometrics

- Authenticate based on unique individual traits.

Processes:

- **Enrollment:** Capture and register biometric data.

- **Verification:** Compare presented biometric data to registered template.

Types:

- **Physiological:** Fingerprints, iris/retina scans, palm scans, venous patterns.
- **Behavioral:** Voiceprint, signature dynamics, keystroke patterns.

Considerations:

- High accuracy but expensive to implement and maintain.
- Privacy concerns and medical information risk.
- Sanitization and hygiene issues with shared devices.

7. Monitoring

Purpose:

Maintain security through surveillance, logging, and alerting.

Monitoring Examples:

- **Cameras:**
  - Integrated with security system, can deter, detect, and provide forensic evidence.
- **Sensors:**
  - Motion detectors (infrared, microwave, lasers), door/gate sensors, vibration sensors on fences.
- **Logs:**
  - Physical and electronic logs record access events.
  - Logs must be securely stored, regularly reviewed, and retained according to policy.
  - Detect anomalies like unexpected access or gaps in logs.
  - Retention driven by business, legal, or regulatory requirements (e.g., PCI DSS).
- **Alarms:**
  - Door/window alarms activate on unauthorized opening.
  - Fire alarms trigger on smoke or heat detection.
  - Panic buttons alert security/police when pressed.
- **Security Guards:**
  - Provide presence to deter tampering, tailgating, or masquerading incidents.
  - Monitor equipment and personnel movement.

8. Logical Access Controls

Definition:

Electronic controls restricting access to systems, applications, and data.

Types Include:

- Passwords
- Biometrics implemented in systems (smartphones, laptops)

- Badge/token readers linked to systems

Purpose:

Limit system access—even when physical access is granted—using electronic authentication and authorization.

Summary:

Layer	Controls Example	Purpose
Physical	Guard, fence, biometrics, locked doors	Prevent unauthorized physical access
Technical/Logical	Firewalls, passwords, MFA, badge readers	Restrict and monitor system/network access
Administrative	Policies, audits, training	Define and enforce security rules
Monitoring	Cameras, sensors, logs, alarms	Detect and respond to security incidents

▼ 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

1. Privileged Access Management (PAM)

Definition and Importance

Privileged Access Management (PAM) refers to the control and monitoring of accounts and identities that have elevated privileges—i.e., permissions that go beyond those of regular users—to access critical systems, applications, and data.

Without PAM, privileged accounts often have persistent access (e.g., admin rights active all the time), which poses significant security risks if compromised. PAM mitigates this by enabling **Just-In-Time (JIT) access**, where elevated permissions are granted only when needed and for a limited time.

How PAM Works

- PAM assigns **role-based specific subsets of privileges**.
- These privileges activate **only at the time of actual resource or service access request**.
- Once no longer needed, privileges are revoked immediately.

Example Scenario: Ransomware Attack

- **Context:** An IT team at ABC, Inc. added their user accounts to the Domain Admins group to simplify tasks.
- **Issue:** They opened a malicious email with ransomware.
- **Result:** Because admin privileges were always on, ransomware encrypted all files on servers and workstations.

- **With PAM:** Elevated access would have been active only during required tasks, limiting ransomware's scope and damage—for example, daily email use done without admin rights.

2. Privileged Accounts

Definition

Privileged accounts hold permissions **beyond normal user levels** and are typically assigned to roles with critical operational responsibilities.

Types of Privileged Accounts and Users

- **System Administrators:** Manage OS, software deployment, performance.
- **Help Desk / IT Support:** Need limited privileged operations, like password resets.
- **Security Analysts:** Require extensive access across infrastructure for monitoring and incident response.
- **Project-specific roles:** Temporary elevated access for particular projects or clients.

Risk and Trust Considerations

- Elevated privileges present risks if misused or abused.
- Trustworthiness and vetting of account holders are essential.

Mitigation Measures

1. **Enhanced Logging:** Detailed activity logs to deter abuse and detect suspicious actions.
2. **Stronger Access Controls:**
    - Multi-factor authentication (MFA) for privileged users.
    - Just-in-time access to restrict privilege use.
3. **Deeper Trust Verification:** Background checks, non-disclosure agreements, financial investigations.
4. **More Frequent Audits:** Continuous or event-triggered monitoring and review.

Practical Example: Help Desk Password Reset

- Help desk staff might only need permissions to reset passwords, often requiring domain admin privileges.
- In PAM, only the **specific permissions needed are granted (password reset and account unlock)**, not full admin rights.
- All password resets are **logged and audited** against support tickets to ensure legitimacy.

3. Authorized Versus Unauthorized Personnel

Key Concepts

- **Authentication:** Confirming the identity of a subject (person/system requesting access).
- **Authorization:** Checking if the authenticated subject has permission to perform the desired action.

How Authorization Works

- Systems maintain a **security matrix** defining access rights.
- Access is granted or denied based on this predefined matrix.

Example 1: Data center door:

- Authorized ID badge opens the door.
- Unauthorized badge does not.

Example 2: File system delete operation:

- User authorized to delete file → file is deleted.
- User not authorized → error message, no deletion.

User Provisioning Processes

1. **New Employee:**
   - Hiring manager requests new user ID with appropriate access.
   - Elevated permissions may require additional authorization.
2. **Change of Position:**
   - Access rights updated according to new job role.
   - Remove access no longer needed.
3. **Separation of Employment:**
   - Accounts disabled post-termination to prevent access.
   - Accounts typically kept disabled for audit trail preservation before deletion.
   - Remove all roles and elevated permissions.

Best Practice: Avoid Permission Creep

- Do **not copy user profiles** when creating new accounts.
- Copying profiles risks inheriting unnecessary permissions—**permission creep**.
- Instead, create users based on **standardized roles** aligned with job functions.

4. Role-Based Access Control (RBAC)

Definition

RBAC assigns access rights and permissions based on defined **roles** within the organization rather than individual users.

How RBAC Works

- **Roles** are created with specific access permissions.
- When a user assumes a job role, they are assigned the corresponding RBAC role.
- If the user leaves or changes roles, permissions associated are removed, reducing risks.

Benefits

- Scales well in environments with frequent staff changes.
- Simplifies access management.
- Ensures users only have access necessary for their job.

5. Role-Based Access Control (RBAC) in the Workplace

Practical Application in Organizations

- **HR Role:** Access to personnel files only.
- **Finance Role:** Access to bank accounts only.
- **Managers:** Access limited to their direct reports and department.
- **System Admins:** Broad access, but still defined by roles.
- **New Employees:** Minimal access based on role requirements.

Challenges: Privilege Creep and Permissions Creep

- Temporary elevation of permissions (e.g., junior staff acting as manager) must be **reverted after the period**.
- Failure to do so leads to **privilege creep** — accumulation of unneeded permissions.
- Managing **multiple, granular roles** demands continuous monitoring and review.

Best Practice Summary:

- Standardized roles should be defined for each job function.
- New users are assigned the role-based default permissions.
- Avoid duplicating actual user profiles to prevent inherited over-privileging.

Summary Table of Key Concepts

Concept	Purpose	Key Features	Examples
Privileged Access Management	Limit and control elevated permissions	Just-in-time access; least-privilege principle; auditing	Restricting admin rights to specific tasks during specific time
Privileged Accounts	Accounts with elevated permissions	Stronger authentication, logging, auditing, trust verification	Help Desk with password reset permission only
Authorized vs Unauthorized	Control who can perform what actions	Authentication, authorization, security matrix	Door badge access; file deletion permissions
Role-Based Access Control	Assign permissions via roles	Central role definition; easy assignment and removal	HR role for personnel files access
RBAC in Workplace	Enforce appropriate access based on role	Prevent privilege creep; standard roles	Temporary permissions for acting managers revoked post use

Access Control Comparison:

Access Control Model	**Definition**	**Example**	**Control Type**	**Flexibility**	**Security Level**	**Common Use Cases**
Discretionary Access Control (DAC)	Resource owners control access and can share permissions freely.	File owner grants read/write access to colleagues.	Decentralized, owner-based	High	Moderate	General user-level access, file sharing

Access Control Model	Definition	Example	Control Type	Flexibility	Security Level	Common Use Cases
Mandatory Access Control (MAC)	Centralized control using strict security labels and clearances.	Only “Top Secret” clearance can access certain documents.	Centralized, policy-based	Low	Very High	Military, government, highly sensitive data
Role-Based Access Control (RBAC)	Access based on predefined organizational roles.	HR accesses personnel files; Finance handles accounting data.	Centralized, role-based	Moderate	Moderate to High	Enterprises with structured job functions
Rule-Based Access Control (RuBAC)	Access granted/denied based on dynamic rules (time, location, etc.)	System access allowed only during business hours or from office.	Centralized, rule-based	High	Moderate to High	Context-aware and time/location-sensitive access
Attribute-Based Access Control (ABAC)	Access decisions use multiple attributes (user, resource, environment).	Access if user is in department X and during work hours.	Centralized, attribute-based	Very High	High	Complex organizations needing fine-grained control
Policy-Based Access Control (PBAC)	Policies evaluate various contextual factors dynamically in real-time.	Allow access only from company devices during office hours.	Centralized, policy-driven	Very High	High	Regulated industries with strict compliance needs