Security Controls Overview

Security controls are safeguards or countermeasures to protect systems, networks, and data from threats. They are categorized by **function** and **type**.

---

1. Security Control Functions

Security controls serve different purposes:

- **Preventive Controls** – Stop incidents before they happen.
  - Firewalls
  - Encryption
  - Access control lists (ACLs)
  - Security awareness training
- **Detective Controls** – Identify incidents after they occur.
  - Intrusion detection systems (IDS)
  - Log monitoring
  - Security audits
  - CCTV surveillance
- **Corrective Controls** – Take action to fix issues after detection.
  - Patching vulnerabilities
  - Incident response plans
  - Restoring from backups
- **Deterrent Controls** – Discourage malicious activity.
  - Warning banners
  - Security guards
  - Security policies
- **Compensating Controls** – Alternative measures when the primary control isn't feasible.
  - Temporary MFA enforcement when biometric access is unavailable
  - Extra logging to compensate for lack of intrusion prevention

---

2. Security Control Types

Security controls are also classified based on implementation:

- **Administrative (Managerial) Controls** – Policies and procedures for security enforcement.
  - Security policies
  - Risk assessments
  - Training and awareness programs
- **Technical Controls** – Use technology to enhance security.
  - Antivirus software
  - Intrusion prevention systems (IPS)

    - Data encryption
- **Physical Controls –** Protect tangible assets from physical threats.
    - Security cameras
    - Badge access systems
    - Biometric scanners