Armaan Shamsaasef

Security Controls

Security Controls - SY0-701 1.1 - Notes

Security controls are safeguards designed to avoid, prevent, detect, or minimize security risks.

---

1. Control Categories (By FUNCTION)

These categories define *what the control does*.

- Managerial: Controls that govern the organization's security policy and procedures.
    - *Focus:* Oversight, risk management, and compliance.
    - *Examples:* Security policies, risk assessments, vendor management.
- Operational: Controls implemented and executed by people (rather than systems).
    - *Focus:* Day-to-day security operations.
    - *Examples:* Security awareness training, configuration management, physical fencing.
- Technical: Controls implemented using technology (hardware, software, or firmware).
    - *Focus:* Automating security.
    - *Examples:* Firewalls, encryption, antivirus software, access control lists (ACLs).

---

2. Control Types (By PURPOSE)

These types define *why the control is used*.

- Preventive: Designed to stop a security incident from *ever* happening.
    - *Examples:* Firewall rules, door locks, security guards, pre-employment drug screening.

- Deterrent: Designed to discourage a violation of security policy by making the target less appealing.
    - *Examples:* "Beware of Dog" sign, visible cameras, warning banners on login screens.
- Detective: Designed to identify and *alert* on a security incident while it is happening or after it has occurred.
    - *Examples:* Intrusion Detection System (IDS), alarm systems, security logs, CCTV monitoring.
- Corrective: Designed to *fix* the impact of an incident and restore normal operations.
    - *Examples:* Restoring data from backups, patching a system, quarantining a virus.
- Compensating: Provides an alternative control when the primary control is not feasible. It offers the same level of protection but in a different way.
    - *Example:* Using a "clean desk policy" (operational) to compensate for the inability to implement full-disk encryption (technical) on all devices.
- Physical: Controls that provide physical protection of facilities, people, and assets.
    - *Examples:* Fences, door locks, biometric access systems, fire suppression systems.

Key Takeaways

- Categories vs. Types: A single control can be described by one Category (Managerial, Operational, Technical) and one Type (Preventive, Deterrent, Detective, etc.).
    - *Example:* A Firewall is a Technical (Category) Preventive (Type) control.
    - *Example:* Security Awareness Training is an Operational (Category) Preventive (Type) control.
- Compensating Controls are about providing equivalent security through a different method when the original control isn't possible.