📘 Domain 1: General Security Concepts (12%)

🔹 1.1 Core Security Principles

🔐 CIA Triad

Principle	Description	Examples
Confidentiality	Ensures that information is accessible only to those authorized.	Encryption, access controls
Integrity	Ensures data has not been altered in an unauthorized way.	Hashing, digital signatures
Availability	Ensures authorized users can access data and systems when needed.	Backups, redundant systems, UPS

> ✅ **IMPORTANT:** Many exam questions ask you to **match a control to a CIA principle**.

🔹 1.2 AAA – Authentication, Authorization, Accounting

✅ Definitions:

- **Authentication** – Verifying a user's identity (e.g., passwords, biometrics).
- **Authorization** – Granting permission to access resources.
- **Accounting** – Tracking and logging user activity (logs, audits).

AAA Protocols:

Protocol	Description
RADIUS	Centralized AAA for remote access; encrypts only passwords.
TACACS+	Encrypts the entire packet; more secure; often used in Cisco environments.
LDAP	Used for directory services; stores user account information.
Kerberos	Uses tickets for authentication; requires time synchronization.

🔹 1.3 Security Control Types

Based on Implementation:

Type	Description	Example
Administrative	Policies, procedures, training	Security awareness training
Technical	Enforced by hardware/software	Firewall, antivirus
Physical	Prevent physical access	Fences, security guards

Based on Purpose:

Type	Purpose	Example
Preventive	Prevent an attack	Firewall, access control
Detective	Detect an attack	IDS, audit logs
Corrective	Restore after attack	Backups, patching
Deterrent	Discourage attack	Warning signs, cameras
Compensating	Alternative control when standard one isn't feasible	Temporary security measures

---

🔹 1.4 Security Roles

Role	Responsibility
Data Owner	Determines access level and classification
Data Custodian	Maintains and protects data
System Owner	Responsible for the security of systems
User	Uses systems and follows policies
Security Admin	Configures and maintains security measures

🔹 1.5 Defense in Depth

Multi-layered approach to security — if one layer fails, others still protect the system.

Layers may include:

- Physical security
- Network security (firewalls, IDS/IPS)
- Host security (antivirus, patching)
- Application security
- Data security (encryption)
- User awareness (training)

  - 🔸 This concept reflects **Zero Trust** and assumes **"breach is inevitable"**.

🔹 1.6 Zero Trust Model

"Never trust, always verify."

- No implicit trust — not even for internal users.
- Enforces strict identity verification for every user and device.
- Often includes:
    - Micro-segmentation
    - Multi-factor authentication
    - Context-aware access

🔸 Very important concept in SY0-701. Expect scenario-based questions.

🔹 1.7 Security Posture

An organization's overall security status and readiness.

Components:

- Asset awareness
- Threat detection
- Risk management policies
- Incident response planning
- Compliance efforts

🔹 1.8 Risk Concepts

Term	Meaning
Risk	Possibility of loss when a threat exploits a vulnerability
Threat	Anything that can cause harm
Vulnerability	Weakness that can be exploited
Exploit	A method used to take advantage of a vulnerability
Likelihood	Chance that a threat will occur
Impact	Potential damage from a threat
Residual Risk	Risk that remains after implementing controls
Risk Appetite	Level of risk an organization is willing to accept

---

📌 Exam Tips for Domain 1

- Understand and **differentiate CIA triad** — expect case studies.
- AAA protocols (RADIUS, TACACS+, LDAP, Kerberos) are high-yield.
- Be able to categorize **security controls** by purpose and type.
- Know how **Zero Trust** differs from traditional models.
- Get comfortable with **risk terminology** — lots of scenario-based questions.
