

Study Guide: General security concepts

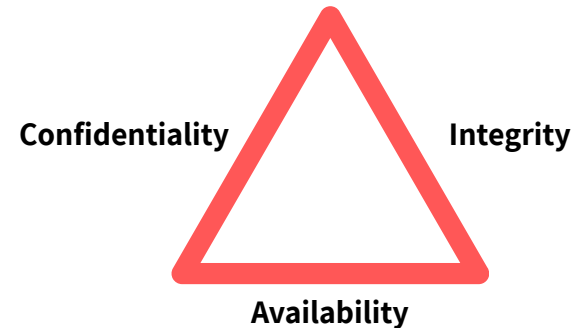
Control Type	Purpose/Function	Nature/Implementation	Example
PREVENTIVE	Stop an undesirable action from occurring	Technical/Managerial/Operational/Physical	Firewall (Technical), Security Policy (Managerial), Locked Door (Physical)
Detective	Identify an undesirable action that has occurred.	Technical/Operational/Physical	Intrusion Detection System (IDS) (Technical), Security Audit/Review (Operational), Surveillance Camera (Physical)
Corrective	Restore systems to their state before an incident.	Technical/Operational	System Backups/Recovery (Technical), Incident Response Plan (Operational)
Deterrent	Discourage potential attackers from attempting an attack.	Managerial/Physical	Security Warning Signs, Visible Cameras, Penalty/Legal Notices
Compensating	Provide an alternative method to meet a security objective when a primary control can't be used.	Technical/Managerial/Operational	Two-factor authentication (2FA) when single sign-on (SSO) is required but lacks strong password policy enforcement.
Corrective	Restore systems to their state before an incident.	Technical/Operational	System Backups/Recovery (Technical), Incident Response Plan (Operational)
Directive	Specify what is acceptable or what must be done.	Managerial	Mandatory Training, Acceptable Use Policy (AUP)

Study Guide: General security concepts

CIA Triad

The foundation of information security:

- **Confidentiality:** Preventing the disclosure of information to unauthorized individuals or systems. (Privacy)
- **Integrity:** Ensuring the accuracy and completeness of data and systems. Preventing unauthorized or accidental modification. (Trustworthiness)
- **Availability:** Ensuring that authorized users have timely and uninterrupted access to systems and information. (Accessibility)



Non-repudiation

The assurance that someone cannot deny the validity of something (e.g., a transaction or a digital signature). It proves the origin of a communication.

Authentication, Authorization, and Accounting (AAA)

- **Authentication:** Verifying the claimed identity (Are you who you say you are? e.g., Username/Password).
- **Authorization:** Determining what an authenticated user can do (What resources can you access? e.g., Permissions/Access rights).
- **Accounting:** Tracking and logging user actions for non-repudiation and auditing purposes (What did you do? e.g., Audit logs).

Zero Trust

A security model based on the principle: "Never trust, always verify."

Core Idea: Assume no user, device, or application—inside or outside the network—is trustworthy by default.

Verification: Access is granted only after strict verification based on context (user identity, device health, service requested).



Study Guide: General security concepts

Change Management

Change management is the structured process for documenting, approving, and implementing changes to an IT environment (software, hardware, network, processes) to minimize disruption and risk.

Business Processes: Understanding how the change impacts overall organizational operations, regulatory compliance, and user workflows. Approval from business owners is crucial.

Technical Implications: Assessing the risks, dependencies, and resources needed for the change (e.g., system downtime, compatibility issues, rollback plan). A technical review board is often involved.

Documentation: All changes must be fully documented, including the reason for the change, the implementation plan, the impact analysis, the testing results, and the rollback procedure.

Version Control: Using a system (like Git, for Linux) to track and manage changes to code, configurations, and documentation. It allows for:

- Reverting to previous, stable versions.
- Tracking who made which change and when.
- Managing concurrent work without conflicts.



Organize ▾				
Name	Publisher	Installed On	Size	Version
Wireshark 4.6.0 x64	The Wireshark developer comm...	11/24/2025	268 MB	4.6.0
Npcap	Nmap Project	11/24/2025		1.78
GNS3	GNS3 Technology Inc.	11/24/2025		2.2.55
Microsoft OneNote - en-us	Microsoft Corporation	11/22/2025		16.0.19328.20244
Microsoft 365 - en-us	Microsoft Corporation	11/22/2025		16.0.19328.20244
Microsoft Edge	Microsoft Corporation	11/21/2025		142.0.3595.94
Google Chrome	Google LLC	11/20/2025		142.0.7444.176

Study Guide: General security concepts

Concept	Description	Key Security Goal
Encryption	Transforming readable data (plaintext) into an unreadable form (ciphertext) using an algorithm and a key.	Confidentiality
Hashing	A one-way mathematical function that takes an input and produces a fixed-size, unique string (hash value or message digest). Cannot be reversed.	Integrity
Digital Signatures	Uses asymmetric cryptography to prove the authenticity and integrity of a document or message. Created using the sender's private key .	Non-repudiation, Integrity, Authentication
Blockchain	A distributed ledger (database) that is decentralized and immutable (cannot be changed). It groups transactions into blocks that are cryptographically linked together in a chain .	Integrity, Non-repudiation, Availability (due to distribution)

Study Guide: General security concepts

Public Key Infrastructure (PKI)

PKI is the framework that manages the creation, distribution, usage, storage, and revocation of digital certificates. It uses asymmetric cryptography (two mathematically linked keys: a public key and a private key).

Key Components:

Certificate Authority (CA): Issues and revokes digital certificates.

Registration Authority (RA): Verifies the identity of the user requesting the certificate.

Digital Certificate: Binds an identity (e.g., a person, server) to a public key.

Certificate Revocation List (CRL): A list of revoked certificates.

