Chapter 1: Security Principles - CC Exam Preparation

# Easy Terminology Definitions

### 🔐 ****CIA Triad (Core Security Concepts)****

**Confidentiality** – Keeping data secret from people who shouldn’t see it.

**Integrity** – Making sure data is not changed without permission.

**Availability** – Ensuring authorized users can access data when they need it.

### 🧠 ****Key Terms in Simple Language****

| **Term** | **Simple Explanation** |
| --- | --- |
| **Authentication** | Proving who you are (like logging in with a password or fingerprint). |
| **Authorization** | Getting permission to access something (like opening a file you’re allowed to see). |
| **Non-repudiation** | No one can deny they did something (e.g., sending a message). |
| **Privacy** | Keeping personal information safe and not shared without consent. |
| **Risk** | The chance that something bad (like a cyberattack) could happen. |
| **Threat** | Anything that could cause harm (e.g., hackers, viruses). |
| **Vulnerability** | A weakness that could be attacked (e.g., outdated software). |
| **Asset** | Something valuable to protect (e.g., computers, data). |
| **Impact** | The damage or harm caused if a risk happens. |
| **Probability** | How likely a risk is to happen. |
| **Risk Management** | Finding and dealing with risks in the best way. |

### 🛠️ ****Security Controls (Ways to Protect Systems)****

| **Type** | **Meaning** | **Examples** |
| --- | --- | --- |
| **Physical Controls** | Protect with physical tools | Locks, security guards, fences |
| **Technical Controls** | Protect with technology | Firewalls, antivirus, encryption |
| **Administrative Controls** | Protect using rules or policies | User access rules, training, audits |

### 🎯 ****Risk Treatment Options****

| **Option** | **What It Means** |
| --- | --- |
| **Accept the risk** | Do nothing, live with it. |
| **Avoid the risk** | Stop the activity causing the risk. |
| **Mitigate the risk** | Reduce the chance or damage. |
| **Transfer the risk** | Pay someone else to take it on (e.g., insurance). |

### 🧑‍💼 ****Governance Elements (Management Tools)****

| **Element** | **Simple Meaning** |
| --- | --- |
| **Policies** | High-level rules made by management. |
| **Standards** | Accepted ways to do things correctly. |
| **Procedures** | Step-by-step instructions. |
| **Regulations** | Legal rules made by governments. |

### 🧬 ****Other Common Terms****

| **Term** | **Simple Meaning** |
| --- | --- |
| **Encryption** | Scrambling data so only authorized people can read it. |
| **Token** | A physical item (like a smart card) used to verify identity. |
| **Biometric** | Using body parts (like fingerprints or eyes) to verify identity. |
| **Bot** | A program that acts automatically, often used by attackers. |
| **GDPR** | A law in Europe that protects people’s private data. |
| **HIPAA** | A U.S. law that protects health information. |
| **Multi-Factor Authentication (MFA)** | Using two or more ways to prove identity (e.g., password + code). |
| **Criticality** | How important something is to your mission. |
| **System Integrity** | Making sure systems run properly without being tampered with. |

# Practice MCQs Based on Chapter 1

1. 1. Which principle of the CIA triad ensures that data is not modified in an unauthorized way?

* A. Confidentiality
* B. Availability
* C. Authorization
* D. Integrity

✅ Correct Answer: D

1. 2. What is the best example of a physical security control?

* A. Firewall
* B. Password policy
* C. Security camera
* D. Antivirus software

✅ Correct Answer: C

1. 3. What does ‘non-repudiation’ ensure in cybersecurity?

* A. Data is not changed
* B. Data is always available
* C. A user cannot deny their actions
* D. Data is hidden from unauthorized users

✅ Correct Answer: C

1. 4. Which of the following is a risk treatment method that involves reducing the chance or impact of a threat?

* A. Avoidance
* B. Mitigation
* C. Transference
* D. Acceptance

✅ Correct Answer: B

1. 5. An attacker exploiting an outdated server software is an example of:

* A. Authentication
* B. Encryption
* C. Threat vector
* D. Security policy

✅ Correct Answer: C

1. 6. What is the main purpose of encryption?

* A. To restrict access to a network
* B. To hide passwords from users
* C. To protect data by making it unreadable without a key
* D. To prevent system downtime

✅ Correct Answer: C

1. 7. Which of the following best describes a standard?

* A. A detailed legal requirement
* B. A broad high-level direction
* C. A best practice used to create policies and procedures
* D. A step-by-step instruction

✅ Correct Answer: C

1. 8. Who is responsible for identifying risks in an organization?

* A. Only the IT department
* B. Only upper management
* C. Only risk analysts
* D. All employees

✅ Correct Answer: D

1. 9. What term is used to describe the lowest acceptable level of security settings?

* A. Encryption
* B. Policy
* C. Baseline
* D. Regulation

✅ Correct Answer: C

1. 10. What type of control is a policy requiring two people to approve a financial transaction?

* A. Technical
* B. Physical
* C. Administrative
* D. Regulatory

✅ Correct Answer: C