# 2.1 Cyber Foundations

Name: _____ Class: _____ Date: _____ **Total: 55 marks**

**KEY WORDS** risk • accept • likelihood • severity • transfer

## Objective

Build the skills to answer exam questions on the **CIA triad** , **social engineering** , **adversaries** , the **phases of an attack** , **risk assessment** , and **security controls** .

**You must be able to:**

- name the seven social-engineering tactics and identify which one a scenario shows
- classify an adversary by motive and capability
- place an action in the correct phase of a cyberattack
- assess a risk from likelihood and severity, and say whether a rating is quantitative or qualitative
- choose a risk response (avoid, transfer, mitigate, accept) and justify it
- classify a control by type *and* by function, and explain why defense in depth is needed

## 1 Key knowledge and worked examples

Study these first. Each one shows the method for a task used later.

### ■ Naming the social-engineering tactic

Ask **what feeling the message manufactures**, not what it claims to be. A pretext is the *cover story*; the tactic is the *pressure*.

> "This is Mr Chen from Finance. The transfer must clear in the next twenty minutes or the auditors will fine the department."

- Claiming to be Finance = **pretexting** (the invented reason for contact).
- Naming a manager to borrow their power = **authority**.
- A twenty-minute deadline = **urgency**.
- Threatening a fine = **intimidation**.

A scenario may show more than one tactic. Quote the words that carry each one; a bare label earns nothing. The defence never changes: **verify through a separate trusted channel** before acting.

### ■ Placing an action in the attack phase

Six phases run in order, and each has one give-away question:

| Phase | The give-away |
|---|---|
| Reconnaissance | still *outside* – reading public (OSINT) information |
| Initial access | first foothold – a phishing click, a stolen password |
| Persistence | keeping the foothold – a RAT, a rootkit, a C2 channel |
| Lateral movement | reaching *further* – escalating privileges, new accounts |
| Taking action | acting on the goal – collecting, exfiltrating, destroying |
| Evading detection | covering up – deleting logs, removing planted files |

*Example.* An adversary already inside a workstation uses a stolen admin password to open the file server. Not initial access – they were already in. Reaching further with higher privilege is **lateral movement**.

### ■ Assessing and rating a risk

Risk needs all three: a **threat** that can exploit a **vulnerability** to compromise an **asset**.

Rate it from two factors, and say what drives each:

- **Likelihood** – the target's *value*, the *skill* needed to exploit it, and the adversary's *motivation and capability*.
- **Severity** – usually financial, but also reputational and operational.

*Example.* A clinic keeps patient records on an unencrypted laptop taken home nightly. Likelihood: **high** – medical data is valuable, and reading an unencrypted disk needs almost no skill. Severity: **high** – a breach carries legal penalties, lost trust and clinic downtime. Rating: **high risk**. That is a *qualitative* rating; "an $80,000 expected annual loss" would be *quantitative*.

### Choosing the risk response

| Response | What it does | When it fails |
|---|---|---|
| Avoid | stop the activity | impossible if the activity is the organisation's purpose |
| Transfer | move the burden (insurer, government, customer) | the reputational damage does not transfer |
| Mitigate | add controls to cut likelihood or impact | never reaches zero |
| Accept | live with what is left | only for **residual risk** you can afford |

An organisation favours controls that are **cost effective** – costing less to install and maintain than the loss they prevent.

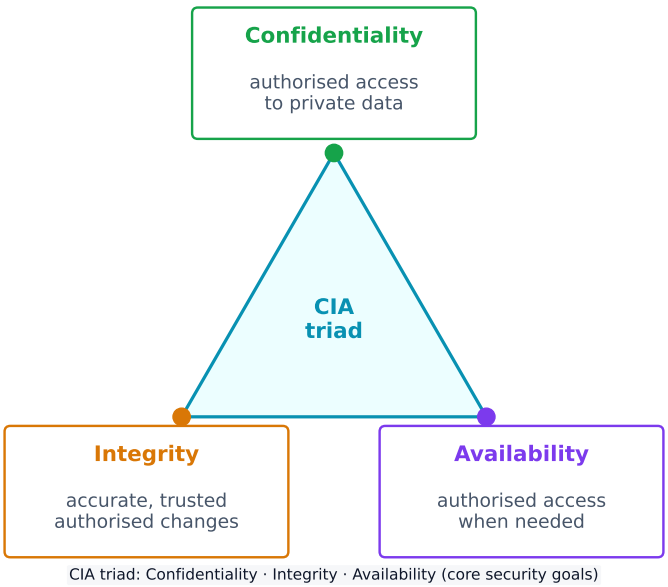
*Example.* The clinic cannot stop treating patients, so avoidance is out. Full-disk encryption is cheap and cuts the likelihood to near zero, so **mitigate**; insurance for the remainder is **transfer**; whatever is left is accepted.

### Classifying a control twice

Every control has a **type** (where it acts) *and* a **function** (what it does), and the exam asks for both.

| | **Preventative** | **Detective** | **Corrective** |
|---|---|---|---|
| **Physical** | door lock, bollard | CCTV camera | repairing a broken card reader |
| **Technical** | firewall, encryption | IDS, SIEM | patching, IPS |
| **Managerial** | password policy | access review | incident response plan |

A camera is **physical** by type and **detective** by function. Reading the row and the column separately is what makes it two marks, not one.



CIA triad: Confidentiality · Integrity · Availability (core security goals)

## 2 Practice

**2.1** State the three goals of the **CIA triad** and give one control that supports each. [6]

**2.2** Name the social-engineering tactic in each message, and quote the words that show it.

(a) "Only three licences left at this price - the offer closes tonight." [2]

(b) "Everyone else on your team has already completed the security form." [2]

(c) "Hi, it's Dan - we met at Priya's leaving lunch. Can you resend that file?" [2]

**2.3** Identify the type of adversary in each case.

(a) A group defaces a mining company's website to publicise its pollution record. [1]

(b) A dismissed employee still holding a valid login copies the client list. [1]

(c) A gang deploys ransomware across hospitals for payment in cryptocurrency. [1]

(d) A teenager runs a downloaded exploit kit, not knowing how it works. [1]

**2.4** Name the phase of a cyberattack shown by each action.

(a) Reading employee job titles from a public networking site. [1]

(b) Installing a remote access trojan so access survives a reboot. [1]

(c) Deleting the server's authentication logs. [1]

(d) Copying the customer database to an external server. [1]

**2.5** Define **risk** in terms of a threat, a vulnerability and an asset, and give **two** examples of an asset that is not physical. [4]

**2.6** A school rates a risk as "likely, high impact". A second school rates the same risk as "$40,000 expected annual loss".

(a) Which rating is qualitative and which is quantitative? [2]

(b) State **one** advantage of the quantitative rating for a governing board. [1]

**2.7** Classify each control by type **and** by function.

(a) A firewall. [2]

(b) A written incident response plan. [2]

(c) A security guard at the server-room door. [2]

(d) Restoring files from backup after ransomware. [2]

## 3 Exam-style questions

**3.1** Encrypting a stored file mainly protects which CIA goal? [1]

- **A** availability
- **B** confidentiality
- **C** integrity
- **D** authority

**3.2** An organisation buys insurance against a cyber loss. Which risk response is this? [1]

- **A** avoid
- **B** transfer
- **C** mitigate
- **D** accept

**3.3** An adversary already has a foothold on one workstation and now escalates privileges to reach the finance server. Which phase is this? [1]

- **A** reconnaissance
- **B** initial access
- **C** lateral movement
- **D** evading detection

**3.4** Which is the best example of a **detective** control? [1]

- **A** a bollard outside the entrance
- **B** a security incident and event management (SIEM) system
- **C** full-disk encryption
- **D** an intrusion prevention system that blocks the connection

**3.5** A regional water utility runs its treatment plant from a control network reachable from the office network. Operators sign in with a shared password that has not changed in four years. An engineer clicks a link in an email claiming to be an urgent regulator notice; malware installs and contacts an outside server nightly.

(a) Identify the social-engineering tactic in the email and quote the words that show it. [2]

(b) Name the phase reached when the malware contacts an outside server nightly, and explain what the adversary gains from it. [2]

(c) Assess the risk to the treatment plant. Refer to **both** likelihood and severity, and justify each from the scenario. [4]

(d) The utility cannot stop treating water. Choose a risk response for the shared password and justify why the other three are unsuitable here. [4]

(e) The utility adds a password policy, network segmentation between office and control networks, and a locked control room. Explain how this illustrates **defense in depth**, naming the layer each control defends. [4]