

Securing Spaces

AP Cybersecurity ■ Unit 2

AP Cybersecurity



What we will cover

- 1 The CIA triad
- 2 Adversaries & attack phases
- 3 Risk & how to manage it
- 4 Classifying controls
- 5 Physical attacks
- 6 Protecting & detecting



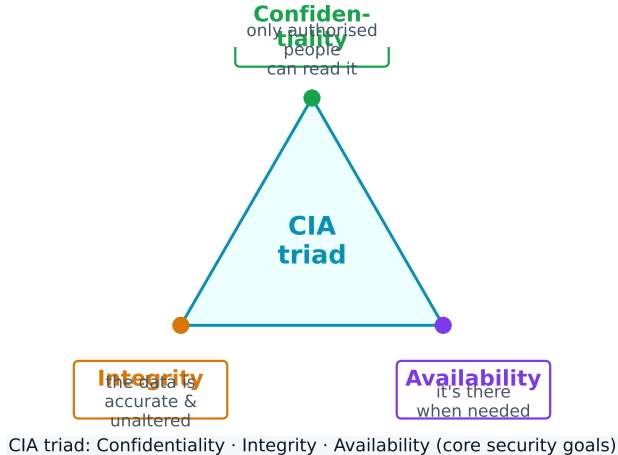
The CIA triad – the three goals of security

Every control protects at least one part of the **CIA triad** :

- **Confidentiality** – only authorised people can read it
- **Integrity** – it is accurate and unaltered
- **Availability** – it is there when needed

Be ready to say which goal a control serves: encryption → confidentiality; a hash → integrity; a backup → availability.

The CIA triad – the three goals of security, in detail



The CIA triad: the three goals every security control supports

Who attacks, and why

Script kiddie

reuses others' tools –
greed or recognition

Hacktivist

a political, social
or personal cause

Insider

already has legitimate access

Cyberterrorist

disrupts critical infrastructure

Transnational criminal organisations chase money – ransomware and stolen data.

Attacks unfold in phases

reconnaissance
– often **OSINT**

initial access,
then persistence

lateral movement

act on the goal,
evade detection



Padlock physical

The phases of an attack

reconnaissance

gathering information, often from public **OSINT** sources – and **dumpster diving**, searching the target's trash

initial access

getting a first foothold – a phished credential, an unpatched service

escalation

raising privileges from that foothold toward administrator

lateral movement

spreading from the first host to others on the network

action on objective

the point of the whole exercise: exfiltrate, encrypt, or destroy

Defences are cheapest at the **early** phases. An attacker stopped at reconnaissance costs nothing; one stopped at exfiltration has already been inside for weeks.

Risk – and the four ways to manage it

A **risk** appears when a **threat** can exploit a **vulnerability** to compromise an **asset** .

Assess it by weighing **likelihood** against **severity** .

Avoid
stop the activity

Transfer
e.g. an insurer

Mitigate
add controls

Accept
live with it

You accept the leftover **residual risk** because perfect security is impossible.

Classifying a control – two ways, always

By type

physical – locks, fences, guards
technical – firewalls, encryption
managerial – policies and procedures

By function

preventative – stop it (a lock)
detective – spot it (a camera)
corrective – fix it (patching)

Exam answers name **both**: a door lock is **physical** by type and **preventative** by function.

Worked example – rate the risk, classify the fix

A hospital stores patient records on an unencrypted server in an unlocked room

The asset is highly sensitive (patient data, protected by law) and the vulnerability is easy to exploit (no encryption, no access control).

⇒ HIGH risk

The fix – a door lock – is physical by type and preventative by function.

High risk needs BOTH high value and easy exploitation. A “foothold to other systems” is the classic moderate risk.

Writing the risk assessment down

what drives likelihood

the value of the target, the skill the exploit needs, and how exposed the vulnerability is

the two ratings

qualitative (low/medium/high – fast, comparable, imprecise) and quantitative (a currency figure – precise, and only as good as its inputs)

a risk assessment records

the vulnerable asset and its value; the likely threats; how the specific vulnerability could be exploited; the likelihood and impact; and the chosen response

the four responses

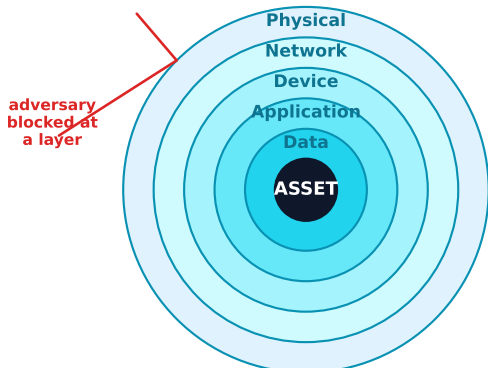
accept, avoid, transfer (insure or outsource), mitigate (add a control)

The exam wants the two rating styles told apart. Qualitative ranks risks against each other; quantitative says what a control is *worth*.

Defence in depth

The best strategy **layers** many controls – **defence in depth** . If an adversary bypasses one layer, **another still stands**. Layers: human, physical, network, device, application, data.

Defence in depth, in detail



The best strategy layers many controls – **defence in depth** . If an adversary gets past one layer, another still stands.

defense in depth: layered controls · one breach must not expose the asset

one breach does not expose the asset



Physical attacks – walking straight in

Digital security means nothing if an adversary can simply walk in. Most **physical attacks** begin with social engineering:

Piggybacking ()
the authorised person
holds the door – tricked

Tailgating ()
slipping through unnoticed

Shoulder surfing
watching you type

Dumpster diving
▪ card cloning

Piggybacking has consent (you were tricked); tailgating does not (you never knew). The exam tests this exact pair.

Protecting physical spaces

Managerial first: security-awareness training (do not badge strangers in) and a workstation policy – locking devices, a **clean desk policy**, privacy screens.

With physical access an adversary can cut power, copy data, or plug in a **key-logger**.

fences, gates, **bollards** – deter

card readers – log and restrict

access control vestibule
– stops piggybacking

disabled **USB** ports; a **UPS**

Detecting physical attacks – placement matters

Some controls **detect** rather than prevent: cameras record, guards respond, **motion sensors** alert – and employees often notice an intruder first.

Cameras belong at **points of ingress and egress** .

Motion sensors work in low-traffic areas like server rooms. Put one in a busy hallway and the constant false alarms make everyone ignore them.

A stationary guard protects a fixed high-value point; a patrolling guard is harder to plan around. Reviewing door-open times can reveal piggybacking – a door held open too long is suspicious.

Protecting Physical Spaces, continued



A dome security camera: physical controls and monitoring protect spaces as well as networks

Cyber Foundations



A monitor wall: network monitoring and logging help detect intrusions

Social engineering: the seven tactics

Most attacks begin not with code but with **social engineering** - psychological tricks that manipulate a person into doing what the adversary wants.

- **quantitative** - a number: a score on a scale (e.g. 1-10), or a money value (e.g. “a \$10,000 annual risk”).
- **qualitative** - a label: *low / medium / high / severe*, or a grid such as *likely-high-impact* vs *unlikely-low-impact*.
- **Avoid** - stop the risky activity (only possible if it isn't essential).
- **Transfer** - shift the burden to someone else, such as an insurer.

The seven social-engineering tactics

pretexting

inventing a believable reason to make contact – “I’m from IT”

authority

posing as someone powerful, or relaying “the boss’s” instructions

intimidation

threatening consequences if a demand is not met

consensus

“everyone in your team has already done this”

scarcity

a limited supply, so hesitating means losing out

urgency

a tight deadline, so the target acts before thinking

familiarity

pretending to be, or to know, someone close to the target

All seven bypass judgement by triggering an **automatic emotional response** – fear, trust, haste, or the wish to fit in. Naming which one an example uses is the exam task.

Exam tips

- Memorise the **CIA triad** and be ready to say *which* goal a control protects - encryption serves **confidentiality**, a hash checks **integrity**, a backup restores **availability**.
- Know the **four risk responses** (avoid, transfer, mitigate, accept) and the two ways to **classify controls** (by type: physical/technical/managerial; by function: preventative/detective/corrective).
- Distinguish **piggybacking** (with consent, tricked) from **tailgating** (without the person's knowledge) - exam questions test this exact pair.
- For risk-rating questions, **high risk needs both high value AND easy exploitation**; a "foothold to other systems" is the classic **moderate** risk.
- **Defense in depth** is the model answer whenever a question asks why one control is not enough.



Unit 2 – key takeaways

1

CIA

say WHICH goal a control serves
– C, I or A

2

Risk

threat × vulnerability on an asset;
avoid, transfer, mitigate, accept

3

Classify twice

by type
(physical/technical/managerial)
AND function

4

Depth

layers – the answer to “why is one control not enough?”

Check yourself

- 1 Which CIA goal does a hash protect?
- 2 Piggybacking or tailgating: the victim knows they let you in?
- 3 Classify a security camera by type and by function.
- 4 Name the four ways to manage a risk.

Answers 1. integrity 2. piggybacking 3. physical; detective 4. avoid, transfer, mitigate, accept