Cyber Security — Chapter study guide

Outcome 2 — Cyber Security · 10 key-knowledge points · exam overview, links & practice

The big picture

Examine the cyber security risks to organisations from insecure software development practices, and recommend strategies to improve the security of software and data.

Unit 4 Outcome 2 examines **cyber security in software development** — how organisations protect data and development practices. It links business goals to security: vulnerabilities, the controls that counter them, threat modelling, evaluation, the law and ethics.

The thread: organisational goals → build in-house or externally → understand vulnerabilities → apply controls → model threats → evaluate security → comply with laws/frameworks → act ethically → mitigate risks → improve practices through training and risk plans.

WHAT THE EXAM REWARDS

- Match a vulnerability (KK03) to the control that mitigates it (KK04) — a very common pairing.
- Threat-modelling's three principles in order, including the final 'confirm mitigated' step.
- Laws vs frameworks: Copyright/Privacy/PDP Acts (must comply) vs Essential Eight/ISM (best practice); know key APPs/IPPs.
- Ethical vs legal issues, and proposing justified mitigation measures for a scenario.
- In-house vs external development trade-offs, including the security/IP angle.

Key knowledge at a glance

KK01	**Goals and objectives of medium and large organisations** Goals and objectives of medium and large organisations.
KK02	**Advantages and disadvantages of developing software in-house or externally** Advantages & disadvantages of in-house vs external software development.
KK03	**Types of vulnerabilities and risks within insecure development environments** Vulnerabilities & risks in insecure development environments.
KK04	**Security controls used to protect development practices and data stored within applications** Security controls: version control/repos, robust IAM, encryption, code review, updates/patches, separated environments.
KK05	**Threat modelling principles** Threat modelling: define security requirements, identify & mitigate threats, confirm mitigation.
KK06	**Criteria for evaluating the security of software development practices within an organisation** Criteria for evaluating the security of an organisation's development practices.
KK07	**Key legislation and industry frameworks affecting how organisations develop software and control data** Key legislation & frameworks: Copyright Act 1968, Essential Eight, ISM, Privacy Act 1988 (APPs), PDP Act 2014 (IPPs).
KK08	**Ethical issues that arise when developing software** Ethical issues in development: ineffective security, AI use, intellectual property, copyright.
KK09	**Mitigation measures to reduce or eliminate threats, vulnerabilities and risks** Mitigation measures to reduce or eliminate threats, vulnerabilities and risks.
KK10	**Strategies for improving the security of software development practices** Strategies for improving secure development: onboarding/training, risk-management plans.

Must-know glossary

Vulnerability	A weakness that could be exploited to cause harm.
Man-in-the-middle attack	A third party secretly intercepting communication between two parties.
Insider threat	Misuse of legitimate access by someone inside the organisation.
Encryption	Encoding data so only authorised parties can read it.
Threat modelling	Defining security requirements, identifying/mitigating threats, and confirming mitigation.
Essential Eight	Eight baseline mitigation strategies recommended by the ACSC (a framework).
Least privilege	Granting only the minimum access each user needs.

Before the exam — revision checklist

- ■ I can distinguish goals from objectives and weigh in-house vs external development.
- ■ I can name and describe the listed vulnerabilities and matching controls.
- ■ I can state the three threat-modelling principles in order.
- ■ I can write measurable criteria to evaluate development security.
- ■ I can distinguish laws from frameworks and apply key APPs/IPPs.
- ■ I can explain the four ethical issues and distinguish ethical from legal.
- ■ I can propose and justify mitigation measures for a given threat.
- ■ I can describe training and risk-management plans as improvement strategies.

Exam practice — questions & model answers

Q1. An organisation stores customer data and lets developers use a shared environment with broad access. Identify two vulnerabilities and a control for each.

Identify · 4 marks

Model answer

• Combined dev/test/prod environment → separate the environments so real data isn't exposed (2).
• Poor IAM (broad access) → robust IAM with least-privilege, role-based access (2).

Q2. State the three principles of threat modelling and why the final one matters.

State/Explain · 4 marks

Model answer

• Define security requirements (1); identify and mitigate threats (1); confirm threats have been mitigated (1).
• The final step verifies the controls actually work, since applying a control doesn't guarantee the threat is removed (1).

Q3. The organisation must protect personal data. Explain one legal obligation (with the principle) and one ethical obligation that apply.

Explain · 4 marks

Model answer

• Legal: under the Privacy Act 1988, APP 11 requires personal data to be kept secure and disposed of when no longer needed (2).

• Ethical: developers have a duty of care to protect users' data well, beyond the legal minimum, e.g. not collecting more than necessary (2).