

KK07 — Key legislation and industry frameworks affecting how organisations develop software and control data

Cyber Security · Comprehensive exam study guide

STUDY DESIGN — YOU MUST KNOW

- Copyright Act 1968 (Cwlth)
- Essential Eight
- Information Security Manual (ISM)
- Privacy Act 1988 (Cwlth) (APP 1, 6, 8, 9, 11)
- Privacy and Data Protection Act 2014 (IPP 1, 2, 4, 5, 9)

You must know the **purpose** of each law/framework and what it requires. Distinguish **laws** (must comply) from **frameworks** (best-practice guidance).

Laws and frameworks

Instrument	Type	Purpose
Copyright Act 1968 (Cwlth)	Law	Protects original works incl. source code from unauthorised copying/use.
Privacy Act 1988 (Cwlth)	Law	Governs handling of personal information via the APPs.
Privacy & Data Protection Act 2014 (Vic)	Law	Governs personal information held by Victorian public bodies via the IPPs.
Essential Eight	Framework	Eight baseline mitigation strategies (by the ACSC) to defend against cyber attacks.
Information Security Manual (ISM)	Framework	ACSC guidance/controls for securing systems and data.

Privacy principles to know

Principle set	Relevant numbers	Cover
APPs (Privacy Act 1988)	1, 6, 8, 9, 11	Open management (1), use/disclosure for purpose (6), overseas disclosure (8), identifiers (9), security (11).
IPPs (PDP Act 2014, Vic)	1, 2, 4, 5, 9	Collection (1), use/disclosure (2), data security (4), openness (5), identifiers (9).

Essential Eight (awareness)

KEY IDEA

The Essential Eight are baseline strategies such as patching applications/operating systems, restricting admin privileges, multi-factor authentication, application control, and regular backups — a recognised framework, not a law.

Key definitions to memorise

Essential Eight	A set of eight baseline cyber-security mitigation strategies recommended by the Australian Cyber Security Centre.
Information Security Manual (ISM)	An ACSC framework providing guidance and controls for securing systems and data.
Australian Privacy Principles (APPs)	Principles in the Privacy Act 1988 (Cwlth) governing handling of personal information.
Information Privacy Principles (IPPs)	Principles in the Victorian PDP Act 2014 governing personal information held by public bodies.

Exam technique

EXAM TIP

- Separate laws (Copyright, Privacy, PDP Acts — must comply) from frameworks (Essential Eight, ISM — best practice).
- Quote a relevant APP (e.g. APP 11 security) or note MFA/patching from the Essential Eight.

COMMON MISTAKES

- Calling the Essential Eight or ISM a 'law' — they are frameworks.
- Mixing APPs (Commonwealth) with IPPs (Victorian).

Quick revision checklist

- I can state the purpose of each law and framework.
- I can match a requirement to the correct instrument and principle.

Exam practice — questions & model answers

Q1. Distinguish between a law and a framework, using examples from this KK.

Distinguish · 2 marks

Model answer

- A law (e.g. the Privacy Act 1988) must be complied with and carries legal consequences (1);
- a framework (e.g. the Essential Eight or ISM) is best-practice guidance that organisations choose to follow (1).

Q2. State which law and principle require an organisation to secure the personal data it stores.

State · 2 marks

Model answer

- The Privacy Act 1988 (Cwlth) (1), under APP 11 (security of personal information) (1).

Q3. Describe the purpose of the Essential Eight.

Describe · 2 marks

Model answer

- It is a set of baseline mitigation strategies (1)
- that help organisations defend against common cyber attacks (e.g. patching, MFA, restricting admin rights, backups) (1).