

Always confirm against the current instrument — CPS 234 paragraph numbers refer to the APRA Prudential Standard, and DISP requirements vary by membership level. This mapping shows where a certified ISMS already does the work.

FRAMEWORK	REFERENCE	OBLIGATION	ISO 27001 CLAUSE / ANNEX A CONTROL	EVIDENCE A PRACTITIONER WOULD PRODUCE
CPS 234	Para 13-14	Board ultimately accountable for information security	Clause 5.1 Leadership and commitment; A.5.2	Board-approved ISMS policy; security a standing board agenda item
CPS 234	Para 15-16	Clearly defined information security roles and responsibilities	Clause 5.3; A.5.2, A.5.4	ISMS Manual role matrix; responsibilities in position descriptions
CPS 234	Para 17-18	Information security capability commensurate with threats	Clause 7.2 Competence; A.6.3	Skills matrix; annual training plan; external DFIR retainer
CPS 234	Para 19-20	Capability of related parties and third parties assessed	A.5.19, A.5.20, A.5.21, A.5.22	Supplier register with annual assurance review; security schedule in MSA
CPS 234	Para 21-22	Information asset identification and classification by criticality and sensitivity	A.5.9, A.5.12	Asset inventory in Intune / Azure Resource Graph; four-tier Purview labels
CPS 234	Para 23-26	Information security controls implemented and commensurate with vulnerabilities	Clause 6.1.3; Annex A (all applicable)	Statement of Applicability; quarterly control testing
CPS 234	Para 27-28	Controls tested for effectiveness through a systematic testing program	Clause 9.1, 9.2; A.5.35, A.5.36	Internal audit programme; annual penetration test; quarterly control tests
CPS 234	Para 29-30	Testing conducted by appropriately skilled and functionally independent parties	Clause 9.2; A.5.35	Internal audit independent of control owners; external assessor annually
CPS 234	Para 31-32	Internal audit reviews the design and effectiveness of information security controls	Clause 9.2	Annual internal audit plan approved by management review
CPS 234	Para 33-34	Robust mechanisms to detect and respond to information security incidents	A.5.24, A.5.25, A.5.26, A.8.16	IR plan with severity model; Sentinel detection; twice-yearly tabletop
CPS 234	Para 35-36	Notify APRA within 72 hours of a material information security incident	A.5.24, A.5.5	IR plan includes a regulator-notification step with the 72-hour clock and named contacts
CPS 234	Para 36	Notify APRA within 10 business days of a material control weakness	Clause 10.1; A.5.36	Nonconformity process flags material weaknesses for regulatory assessment
DISP	Governance	Security officer appointed; security governance documented	Clause 5.3; A.5.2	Named Chief Security Officer; governance documented in the ISMS Manual
DISP	Personnel	Personnel security clearances and screening appropriate to level	A.6.1, A.6.2	Background checks; AGSVA clearances held where the contract requires
DISP	Physical	Physical security certified to the required zone	A.7.1-A.7.4	Office zoning and access control; Azure inherited controls evidenced by Microsoft attestations
DISP	ICT	ICT systems accredited and operated to the PSPF / ISM baseline	A.8.1-A.8.34	Control set mapped to the ACSC Essential Eight and the ISM; evidence retained per control
DISP	Entry Level	Demonstrate a working information security capability	Clause 4-10 (full ISMS)	A certified ISO 27001 ISMS is the most common evidence accepted at Entry Level