Aegentra
ACADEMY

AS ISO 31000:2018 mapped to Australian risk obligations

APRA CPS 220 / 230 / 234, the SOCI Act, the PSPF, Comcover, ASX Principle 7, WHS and the Privacy Act

No Australian law mandates ISO 31000, but several regimes require exactly what it produces. Always confirm against the current instrument — APRA prudential standards, the PSPF and the SOCI Act rules are amended periodically and paragraph numbering changes.

REGIME	WHO IT APPLIES TO	OBLIGATION	AS ISO 31000:2018 REFERENCE	WHAT THE STANDARD GIVES YOU	EVIDENCE TO RETAIN
APRA CPS 220 Risk Management	APRA-regulated institutions	Maintain a risk management framework proportionate to the size and complexity of the institution	Clause 5 — Framework	The framework structure: leadership and commitment, integration, design, implementation, evaluation, improvement	Board-approved risk management framework document with version history
APRA CPS 220 Risk Management	APRA-regulated institutions	Board-approved risk appetite statement setting the level of risk the institution is willing to accept	Clause 6.3.4 — Risk criteria	Risk criteria defined before assessment; appetite expressed as thresholds rather than adjectives	Risk appetite statement with escalation thresholds and board minutes approving it
APRA CPS 220 Risk Management	APRA-regulated institutions	Annual declaration to APRA on risk management	Clause 6.6 — Monitoring and review	A defined review cycle producing evidence the framework was assessed, not merely operated	Annual review report and the resulting improvement actions
APRA CPS 230 Operational Risk Management	APRA-regulated entities	Identify and assess operational risks and maintain effective internal controls	Clause 6.4 — Risk assessment	Identification, analysis and evaluation as three distinct steps, with control effectiveness assessed rather than assumed	Operational risk register with control effectiveness ratings and testing dates
APRA CPS 230 Operational Risk Management	APRA-regulated entities	Identify critical operations and set tolerance levels for disruption	Clause 6.3.4 — Risk criteria	Tolerance expressed as a measurable threshold per consequence type	Critical operations list with maximum tolerable disruption periods
APRA CPS 230 Operational Risk Management	APRA-regulated entities	Manage risks arising from service providers	Clause 6.4.2 — Risk identification	Systematic identification extending beyond the organisation's own boundary	Service provider register with criticality ratings and substitutability assessment
APRA CPS 234 Information Security	APRA-regulated entities	Classify information assets by criticality and sensitivity	Clause 6.4.2 — Risk identification	A repeatable method for identifying what is at risk before assessing how much	Information asset register with classification and owner
APRA CPS 234 Information Security	APRA-regulated entities	Maintain information security controls proportionate to the threat	Clause 6.5 — Risk treatment	Treatment selection justified against criteria rather than chosen ad hoc	Treatment plans with residual risk accepted by a named owner
SOCI Act — Critical Infrastructure Risk Management Program	Responsible entities for critical infrastructure assets across the designated sectors	Establish and maintain a written Risk Management Program addressing all hazards — cyber, personnel, supply chain and physical	Clause 5.4 — Implementing the framework	A single framework covering every hazard category rather than separate silos	Written CIRMP with the four hazard vectors addressed and dated
SOCI Act — Critical Infrastructure Risk Management Program	Responsible entities for critical infrastructure assets	Annual report to the board and to the regulator on the Risk Management Program	Clause 6.6 — Monitoring and review	Review as a defined activity with outputs, not a standing agenda item	Annual CIRMP report with board approval recorded
SOCI Act — Critical Infrastructure Risk Management Program	Responsible entities for critical infrastructure assets	Identify material risks to the availability, integrity, reliability and confidentiality of the asset	Clause 6.4.2 — Risk identification	Identification driven by objectives and consequence types rather than by a control checklist	Hazard register mapped to the asset and its critical functions
PSPF — Protective Security Policy Framework	Australian Government non-corporate Commonwealth entities	Determine and manage security risks using a risk management approach	Clause 6 — Process	The full process: scope and context, identification, analysis, evaluation, treatment, monitoring, communication	Security risk assessment following a documented method
PSPF — Protective Security Policy Framework	Australian Government entities	Accountable Authority annually attests to the entity's security maturity	Clause 5.7 — Improvement	A framework that produces maturity evidence over time rather than a point-in-time snapshot	Annual attestation with supporting maturity assessment

REGIME	WHO IT APPLIES TO	OBLIGATION	AS ISO 31000:2018 REFERENCE	WHAT THE STANDARD GIVES YOU	EVIDENCE TO RETAIN
Commonwealth Risk Management Policy	Commonwealth entities under the PGPA Act	Establish and maintain appropriate systems of risk oversight, management and internal control	Clause 5 — Framework	The framework as the system of oversight, with accountability defined at each level	Risk management policy and framework endorsed by the Accountable Authority
Commonwealth Risk Management Policy	Commonwealth entities under the PGPA Act	Embed systematic risk management into business processes	Clause 5.5 — Integration	Integration treated as a design requirement rather than an afterthought	Evidence risk assessment is a required step in planning and procurement processes
Comcover Risk Management Benchmarking	Commonwealth entities insured through Comcover	Annual benchmarking of risk management maturity	Clause 6.6 — Monitoring and review	A review cycle producing comparable year-on-year evidence	Benchmarking submission and the improvement plan arising from it
ASX Corporate Governance Principles — Principle 7	ASX-listed entities	Establish a sound risk management framework and periodically review its effectiveness	Clause 5.6 — Evaluation	Evaluation of the framework itself, distinct from evaluation of individual risks	Board or committee review of framework effectiveness with findings
ASX Corporate Governance Principles — Principle 7	ASX-listed entities	Disclose whether the entity has a risk committee and how risk is overseen	Clause 5.3 — Roles and responsibilities	Explicit allocation of risk accountability across board, executive and business	Charter of the Audit and Risk Committee and the risk accountability matrix
WHS Act and Regulations	All persons conducting a business or undertaking	Eliminate or minimise risks to health and safety so far as is reasonably practicable	Clause 6.5 — Risk treatment	Treatment options considered in order, with the reasoning recorded	Hazard assessments showing options considered and why the chosen control was reasonably practicable
Privacy Act — Australian Privacy Principle 11	APP entities	Take reasonable steps to protect personal information from misuse, interference and loss	Clause 6.4.3 — Risk analysis	Analysis separating likelihood from consequence so 'reasonable steps' can be justified	Privacy risk assessment with the reasoning for the steps taken