

Risk Management Framework

The parent framework that sets how an organisation governs, assesses, rates, controls, monitors and reports risk, with one common rating scale and language. Ready to adapt for your organisation.

Version 1.0 · October 2026 · Free template from Risk Frameworks Australia (riskfa.com) · No membership or sign-up

How to use this industry framework. This is the parent document of the RiskFA set: every other RiskFA policy, standard, plan and statement uses its rating scale, risk categories and terms. Adopt the structure, terms and ratings as written, so that your organisation speaks the same language as the rest of the industry. Fill in the text in [square brackets] with your organisation's details, calibrate the thresholds to your size and risk appetite, delete obligations that do not apply to you, and approve the Framework through your governance process. Regulatory requirements are summarised as at October 2026: confirm the current requirements that apply to your organisation before relying on them. This template is general information only, provided free of charge, and is used at your own risk (see the disclaimer at the end).

Document control

Item	Detail
Document	Risk Management Framework
Organisation	[Organisation name]
Document owner	[Chief Risk Officer]
Approved by	[Board], on the recommendation of the [Board Risk Committee]
Version / date approved	[1.0] / [date]
Review cycle	At least [annually], and after any material change in strategy, business mix, regulation or risk profile
Related Board-approved documents	the RiskFA Risk Appetite Statement, [Risk Management Strategy] (APRA-regulated entities), [Business Plan]

1. Purpose

This Framework sets out how [Organisation] identifies, assesses, manages, monitors and reports the risks that could affect its objectives, its customers and the community. It ensures that:

- the Board sets the amount and type of risk the organisation is willing to accept, and management operates within it;
- every material risk has an owner and effective controls;
- risks are rated on one common scale, so that they can be compared, aggregated and reported consistently;
- the Board and management receive accurate and timely information on the risk profile; and
- the organisation meets its legal and regulatory risk management obligations.

The Framework supports [Organisation] 's obligations, where they apply, under APRA Prudential Standards CPS 220 *Risk Management* or SPS 220 *Risk Management*, CPS 230 *Operational Risk Management*, CPS 510 / SPS 510 *Governance*, the *Financial Accountability Regime Act 2023* (FAR) and, for Australian financial services (AFS) licensees, the obligation in *Corporations Act 2001* s912A(1)(h) to maintain adequate risk management systems. It follows the principles, framework and process of AS ISO 31000:2018 *Risk management — Guidelines*.

2. Scope and application

This Framework applies to all employees, contractors, directors and officers of [Organisation] and its subsidiaries, to all business units, products, services, systems and locations, and to risks arising from service providers and other third parties. CPS 220 para 20 describes the risk management framework as the totality of systems, structures, policies, processes and people that identify, measure, evaluate, monitor, report and control or mitigate all internal and external sources of material risk; SPS 220 para 6 uses similar wording (identify, assess, manage, mitigate and monitor). This document is the top of that framework.

If [Organisation] is	Main risk management requirements (as at October 2026)
An ADI, general insurer, life company, private health insurer or authorised NOHC	CPS 220 (risk management framework, risk appetite statement, risk management strategy, business plan, CRO, reviews, declaration); CPS 230; CPS 510 (Board Risk Committee, internal audit); FAR (ADIs from 15 March 2024; insurers from 15 March 2025).

If [Organisation] is	Main risk management requirements (as at October 2026)
An RSE licensee (superannuation trustee)	SPS 220 (equivalent requirements, adapted for beneficiaries); CPS 230 (which applies to RSE licensees); SPS 510; SPS 515 for strategic and business planning; FAR (from 15 March 2025).
An AFS licensee not regulated by APRA (including responsible entities and corporate directors of CCIVs)	Corporations Act s912A(1)(h): adequate risk management systems. ASIC guidance: RG 104 (RG 104.59–RG 104.66) for all AFS licensees, and RG 259 <i>Risk management systems of fund operators</i> for responsible entities of registered schemes and corporate directors of CCIVs.
Another financial services business (for example a credit licensee or non-licensed provider)	No single prescribed framework. Adopt this Framework as good practice, scaled to the nature, size and complexity of the business.

CPS 220 does not apply to RSE licensees (CPS 220 para 2 and footnote 1): they apply SPS 220. The s912A(1)(h) risk management systems obligation does not apply to a body regulated by APRA, except an RSE licensee that is also the responsible entity of a registered scheme (and then not to risks relating solely to operating a regulated superannuation fund) (*Corporations Act 2001* s912A(5); RG 104, Table 1); APRA's prudential standards apply instead.

3. The core idea

Risk appetite + effective controls = management of risk. Everything else in this Framework, and in every other RiskFA document, is how we speak about, document and report it.

- **Risk appetite** says how much risk, and what type, the organisation is willing to accept in pursuit of its objectives. The Board sets it, and risk tolerances and limits make it measurable (section 9).
- **Effective controls** keep each risk within appetite. A control is effective only when it is both well designed and operating as intended, and the organisation knows this because it monitors and tests it (section 12). CPS 230 para 15(c) requires internal controls that are designed and operating effectively for the management of operational risks.
- **The common language** (taxonomy, rating scale, glossary) and **the reporting** (RCSA, KRIs, incidents and issues, Board reports) show whether the organisation is within appetite and whether its controls work.

When a risk moves outside appetite, or a control is found not to work, the response is always the same: escalate, act to bring the risk back within appetite, and fix the control at its root

cause.

4. Principles

The Framework applies the risk management principles in AS ISO 31000:2018 clause 4. Risk management at [Organisation] is:

1. **Integrated** into strategy, planning, decision-making and everyday operations, not run as a separate exercise.
2. **Structured and comprehensive**, using one process, one taxonomy and one rating scale across the organisation.
3. **Customised** to [Organisation] 's objectives, size, business mix and complexity.
4. **Inclusive**: the people who own and run the business are involved, and stakeholders' views are taken into account.
5. **Responsive to change**: risks, controls and appetite are reviewed as the business, the market, technology and threats change.
6. **Based on the best available information**, including data, experience, incidents, expert judgement and forward-looking analysis, with its limitations understood.
7. **Aware of human and cultural factors**: behaviour and culture affect every part of risk management.
8. **Continually improved** through learning from incidents, issues, reviews and testing.

5. Risk governance and the three lines of accountability

The Board is ultimately responsible for the risk management framework and for overseeing its operation by management (CPS 220 para 9; SPS 220 para 7). [Organisation] uses three lines of accountability, so that every risk has an owner, independent challenge and independent assurance.

Line	Who	Responsibilities
First line	Business units, product and operations owners, technology, and the executives who lead them	Own and manage risk: identify and assess risks, design and operate controls, monitor KRIs, record incidents and issues, and act to stay within appetite. Senior management are responsible for operational risk management across the end-to-end process (CPS 230 para 23).

Line	Who	Responsibilities
Second line	Risk and Compliance, led by the CRO and the Head of Compliance	Own this Framework and the risk policies; set methods and tools; review and challenge first line risk assessments, ratings and control effectiveness; monitor the risk profile against appetite; report independently to the executive and the Board. The risk management function must be operationally independent (CPS 220 para 37; SPS 220 para 24) and the compliance function must have a reporting line independent from business lines (CPS 220 para 43).
Third line	Internal Audit	Provide independent assurance to the Board Audit Committee on the adequacy and effectiveness of risk management, governance and controls, including this Framework (CPS 510 paras 68–69; SPS 510 para 38).

5.1 Board and committee structure

Body	Role in risk management
Board	Approves this Framework, the Risk Appetite Statement, the Risk Management Strategy and the business plan; forms a view of risk culture; oversees the risk profile against appetite.
Board Risk Committee	Provides objective non-executive oversight of the implementation and operation of the risk management framework. For ADIs and insurers (other than foreign ADIs and Category C insurers) it is mandatory, with at least three non-executive directors, a majority independent, and an independent chair who is not the Board chair (CPS 510 paras 79–83). Its charter covers the matters in CPS 510 para 84. For RSE licensees SPS 510 requires a Board Audit Committee (para 24) but not a Board Risk Committee; a Board Risk Committee is good practice.
Board Audit Committee	Receives the annual review of compliance with, and effectiveness of, the risk management framework (CPS 220 para 44) and oversees Internal Audit.
[Executive Risk Committee]	Chaired by the [CEO]. Reviews the enterprise risk profile, appetite breaches, emerging risks, key control failures and significant incidents and issues before they go to the Board Risk Committee. [Monthly].
[Specialist committees]	For example [Asset and Liability Committee], [Credit Committee], [Investment Committee], [Operational Risk and Compliance Committee], [Technology and Cyber Risk Committee]. Each has a charter, reports to the Executive Risk Committee and applies this Framework.

6. Roles and responsibilities

Role	Responsibilities
Board	Ultimately responsible for the risk management framework (CPS 220 para 9; SPS 220 para 7). Sets risk appetite and approves the Risk Appetite Statement and Risk Management Strategy; forms a view of risk culture and ensures desirable changes are made (CPS 220 para 9(b)); ensures sufficient resources are dedicated to risk management; oversees operational risk and the effectiveness of key internal controls (CPS 230 paras 19–21); makes the annual risk management declaration (CPS 220 para 49; SPS 220 para 32).
Board Risk Committee	Advises the Board on current and future risk appetite and the risk management strategy; oversees the risk position against appetite and capital strength; constructively challenges management; sets the CRO's objectives, reviews performance and endorses appointment or removal (CPS 510 paras 84–85); recommends this Framework to the Board.
Chief Executive Officer and executive team	Run the business within risk appetite; own the material risks in their areas; ensure controls are designed and operating effectively; set the tone for risk culture; provide the Board with clear information on risk, including the expected impact of decisions on critical operations (CPS 230 para 22).
Accountable persons (FAR, where applicable)	Meet their accountability obligations under FAR Act s21 in their areas of responsibility, including taking reasonable steps to prevent matters that would adversely affect the entity's prudential standing or prudential reputation and to prevent material contraventions of the relevant laws. Reasonable steps include having appropriate governance, control and risk management (s22). Their responsibilities are set out in accountability statements and the accountability map (ss33–34).
Chief Risk Officer	Leads the risk management function and owns this Framework. Is involved in, and has authority to provide effective challenge to, decisions that may materially affect the risk profile (CPS 220 para 38). Is independent from business lines, revenue-generating responsibilities and finance, and is not the CEO, CFO, Appointed Actuary or Head of Internal Audit (para 39). Reports directly to the CEO with regular and unfettered access to the Board and Board Risk Committee (para 40).

Role	Responsibilities
Head of Compliance / General Counsel	Leads the compliance function; maintains the obligations register; advises on legal and regulatory risk; manages breach assessment and regulatory notifications under the RiskFA Incident & Issues Management Standard.
Chief Information Security Officer (CISO)	Leads information security risk management in line with CPS 234 and this Framework.
Chief Technology Officer	Owns technology risk, including the age and health of information assets and the IT capability needed to support critical operations (CPS 230 para 24).
Head of Internal Audit	Provides independent assurance on this Framework and on the design and operating effectiveness of controls; delivers or commissions the annual audit review (CPS 220 para 44).
Risk owner	A named senior person accountable for managing a risk within appetite: keeps its assessment current, makes sure controls and actions are in place, monitors its KRIs and escalates when it moves outside appetite.
Control owner	Accountable for designing, operating and evidencing a control, and for reporting when it is not working.
Incident, Issue and Action owners	As defined in the RiskFA Incident & Issues Management Standard.
All staff	Understand the risks in their role; follow policies and controls; speak up about risks, incidents, near misses and control weaknesses.

7. The document hierarchy

Risk management documents fit in one hierarchy. A lower document must not conflict with a higher one. Appendix E shows the hierarchy in full.

Level	Document	Purpose	Approved by
1	Risk Management Framework (this document), Risk Appetite Statement, [Risk Management Strategy], [Business Plan]	How risk is governed and how much risk the organisation will accept	[Board]

Level	Document	Purpose	Approved by
2	Policies (for example Operational Risk Management, Compliance, Information Security, Third Party, Credit, Liquidity)	What must be achieved for a risk category, and who is accountable	[Board or Board Risk Committee]
3	Standards (for example the Incident & Issues Management Standard)	Minimum requirements and methods that apply across the organisation	[CRO or Executive Risk Committee]
4	Procedures, guidelines and work instructions	How a task is done in a business unit	[Business unit head], with second line review

- Every document has an owner, an approval date, a next review date and the person responsible for the review. APRA-regulated entities must monitor these dates for risk management policies and procedures (CPS 220 para 36; SPS 220 para 22(b)).
- For an APRA-regulated entity, the **Risk Management Strategy** is a Board-approved document that describes each material risk, the approach to managing it, the risk policies and procedures, the role of the risk management function, the governance relationships and the approach to risk awareness and risk culture (CPS 220 paras 29–30; SPS 220 paras 21–22). This Framework can form the core of the Risk Management Strategy if it contains all of those elements; Appendix F maps them.
- Exemptions from a policy or standard must be approved in writing by the document owner and the CRO, time-limited, and recorded as an issue or risk acceptance.

8. Risk taxonomy

The RiskFA Risk Taxonomy (riskfa.com/taxonomy) publishes these categories with a stable code for every Level 2 risk type (for example OPS-CYB, Information security and cyber), and links each risk type to the RiskFA standards that manage it and the obligations that apply. Use the codes in your risk register.

[Organisation] classifies every risk, incident, issue and control against one taxonomy, so that risks can be aggregated and reported consistently. The Level 1 categories cover the material risks listed in CPS 220 para 26 and SPS 220 para 12, and the operational risks listed in CPS 230 para 23. Delete the categories that do not apply to you; keep the names of those that do.

Level 1 category	Level 2 risk types (codes)	Definition
Strategic (STR)	STR-BUS Business model and strategy; STR-CMP Competition and market change; STR-CAP Capital planning; STR-MNA Mergers, acquisitions and major investments	The risk that the organisation's strategic objectives, business plan or business model fail or are not achieved, including risks arising from changing those plans.
Financial: credit (CRD)	CRD-DEF Counterparty default; CRD-CON Credit concentration; CRD-QLT Credit quality and lending standards; CRD-COL Collateral	The risk of loss from a borrower or counterparty failing to meet its obligations.
Financial: market and investment (MKT)	MKT-IRB Interest rate risk in the banking book; MKT-TRD Traded market risk; MKT-INV Investment performance; MKT-FX Foreign exchange	The risk of loss, or of poor outcomes for members, from movements in market prices, rates or investment values.
Financial: liquidity (LIQ)	LIQ-FND Funding; LIQ-INV Liquidity of investment options; LIQ-COL Collateral and margin calls	The risk of being unable to meet obligations, including payments to depositors, policyholders or members, as they fall due.
Financial: insurance (INS)	INS-UWP Underwriting and pricing; INS-RES Reserving; INS-REI Reinsurance; INS-MEM Insurance for members	The risk of loss from inadequate pricing, reserving or claims experience, or (for RSE licensees) from insurance arrangements for members.
Operational (OPS)	OPS-PRC Process execution; OPS-PPL People; OPS-TEC Technology; OPS-CYB Information security and cyber; OPS-DAT Data; OPS-CHG Change management; OPS-TPR Third party and service provider; OPS-FRD Fraud (internal and external); OPS-BCM Business continuity; OPS-AI Artificial intelligence and models; OPS-LEG Legal	The risk of loss from inadequate or failed internal processes or systems, the actions or inactions of people, or external drivers and events (drawn from CPS 230 para 12).

Level 1 category	Level 2 risk types (codes)	Definition
Compliance and regulatory (CMP)	CMP-LIC Licence and prudential obligations; CMP-BRP Breach and regulatory reporting; CMP-FCR Financial crime (AML/CTF, sanctions); CMP-PRV Privacy; CMP-DIS Market disclosure; CMP-TAX Tax; CMP-WHS Work health and safety	The risk of failing to comply with laws, regulations, licence conditions, industry codes or internal policies.
Conduct (CON)	CON-PDD Product design and distribution; CON-SAL Sales practices; CON-ADV Advice; CON-CMP Complaints handling; CON-VUL Vulnerable customers; CON-COI Conflicts of interest; CON-REM Customer remediation	The risk that the behaviour of the organisation or its people causes poor outcomes for customers or members, or damages market integrity.
Governance and accountability (GOV)	GOV-BRD Board and governance; GOV-RMF Risk management framework; GOV-ACC Accountability; GOV-REM Remuneration; GOV-CUL Risk culture and consequence management; GOV-FNP Fit and proper; GOV-WBL Whistleblowing; GOV-INV Investment governance (superannuation)	The risk that governance, accountability, remuneration or culture fail to support sound risk management. Includes the governance and investment governance risks required by SPS 220 para 12(a) and (b) for RSE licensees.
Reputational (REP)	REP-STK Stakeholder trust	The risk of loss of trust or standing with customers, members, regulators, investors or the community. Usually a consequence of other risks.
Climate and sustainability (CLM)	CLM-PHY Physical risk; CLM-TRN Transition risk; CLM-LIA Liability risk; CLM-NAT Nature-related risk	The risk of loss or harm from climate change and the transition to a low-carbon economy. Usually acts through other categories.

Artificial intelligence risk sits within operational risk (models, data, technology, third party and conduct). No Australian prudential standard specific to AI applied as at October 2026; manage it with the existing controls for models, data, change, service providers and information security, and record it as its own Level 2 risk type so it can be reported.

9. Risk appetite

Risk appetite is the amount and type of risk [Organisation] is willing to accept in pursuit of its objectives. It is set by the Board and written in the RiskFA Risk Appetite Statement. **Risk tolerances / limits** are the measurable boundaries that put appetite into practice.

For APRA-regulated entities the Risk Appetite Statement must, at a minimum, convey (CPS 220 para 28; SPS 220 para 20):

- the degree of risk the entity is prepared to accept in pursuit of its strategic objectives and business plan, giving consideration to the interests of depositors, policyholders or beneficiaries (risk appetite);
- for each material risk, the maximum level of risk the entity is willing to operate within, expressed as a risk limit (risk tolerance);
- the process for ensuring that risk tolerances are set at an appropriate level, based on the impact if a tolerance is breached and the likelihood that each risk is realised;
- the process for monitoring compliance with each risk tolerance and taking action if it is breached; and
- the timing and process for review of the risk appetite and risk tolerances.

CPS 230 para 15(b) also requires an assessment of the operational risk profile with a defined risk appetite supported by indicators, limits and tolerance levels. AFS licensees that operate funds should document risk appetite and a risk tolerance for each material risk in a policy or statement approved by the board or its delegate (RG 259.21(e), RG 259.32–RG 259.34).

9.1 How appetite is used

- **Cascade.** Board-level appetite statements and metrics are cascaded into limits for business units, portfolios and risk types, owned by named executives.
- **Decisions.** Strategy, business plans, new products, major changes and material service provider arrangements must show their effect on the risk profile against appetite (CPS 220 para 33; CPS 230 para 25).
- **Monitoring.** Each appetite metric has an early warning trigger and a tolerance limit, monitored through KRIs (section 14).
- **Breaches.** A tolerance or limit breach is escalated by the risk owner to the CRO within [24 hours], and by the CRO to the Board Risk Committee chair within [2 business days], with an action plan to return within appetite (RiskFA Risk Appetite Statement section 17). Breaches are recorded as issues under the RiskFA Incident & Issues Management Standard.
- **Review.** The Risk Appetite Statement is reviewed at least [annually] and when strategy or the external environment changes materially.

10. The risk management process

[Organisation] follows the risk management process in AS ISO 31000:2018 clause 6. It applies to enterprise risks, business unit risks, projects, change, new products and individual decisions.

Step (AS ISO 31000 clause)	What must happen at [Organisation]
1. Communicate and consult (6.2)	Involve the people who own, run and are affected by the activity, and the relevant second line specialists, at every step. Share risk information openly across business units.
2. Establish scope, context and criteria (6.3)	Define the objective or activity being assessed, the internal and external context (strategy, obligations, customers, technology, service providers, threats), and the criteria: the risk appetite and the rating scale in this Framework.
3. Identify risks (6.4.2)	Find, recognise and describe risks that could help or prevent the achievement of objectives. Use workshops, process maps, obligations registers, incident and issue data, complaints, audit findings, scenario analysis, emerging risk scans and external loss data. Describe each risk as cause, event and consequence.

Step (AS ISO 31000 clause)	What must happen at [Organisation]
4. Analyse risks (6.4.3)	Understand the causes, the existing controls and how effective they are, and rate the likelihood and consequence using section 11 and the appendices.
5. Evaluate risks (6.4.4)	Compare the residual rating with risk appetite to decide whether the risk is acceptable or needs treatment, and how urgently.
6. Treat risks (6.5)	Select and implement treatment: avoid the risk (stop the activity), reduce likelihood or consequence (new or improved controls), share it (insurance, contracts), or accept it within appetite. Treatments are actions with owners and due dates. Risks outside appetite must be treated, or accepted only under section 18.
7. Monitor and review (6.6)	Monitor risks, controls, KRIs and the external environment continuously; reassess risks at least [annually] and when a trigger in section 13 occurs.
8. Record and report (6.7)	Record every risk, control, assessment and treatment in the [GRC system / risk register] . Report to management and the Board under section 20.

Every risk in the register records at least: ID and title; description (cause, event, consequence); taxonomy category; risk owner; inherent rating; linked controls and their effectiveness; residual rating; target rating and treatment actions; linked KRIs, incidents and issues; appetite status; and the date of the last review.

11. Rating risks

All risks are rated on the RiskFA common rating scale: **Critical, High, Medium, Low**. The same scale is used for risks, incidents and issues, so that a High risk and a High incident mean the same level of concern.

11.1 How to rate a risk

1. Rate the **consequence** on each of the six impact categories in Appendix B: Financial; Customers; Regulatory and legal; Operations and critical operations; Information security and privacy; Reputation. Use the realistic worst case, not the worst imaginable case. The consequence level is the **highest** reached in any one category.
2. Rate the **likelihood** of that consequence occurring over the next **[12 months]**, using Appendix C.
3. Read the rating from the 5×5 matrix in Appendix A.
4. Record the reasons for each rating, the information relied on and its limitations (CPS 220 para 9(g) requires the Board to recognise the uncertainties, limitations and assumptions in measuring material risks).

Incidents have already happened, so they are rated on consequence alone: Severe = Critical, Major = High, Moderate = Medium, Minor or Insignificant = Low. The descriptors for Severe, Major, Moderate and Minor in Appendix B are the same as the Critical, High, Medium and Low thresholds in section 8 of the RiskFA Incident & Issues Management Standard. **Issues** are rated on likelihood and consequence of harm if the weakness is not fixed.

11.2 Inherent, residual and target risk

Rating	Meaning
Inherent risk	The rating before taking account of controls (or assuming the controls fail). Shows how much the organisation depends on its controls and which controls are key.
Residual risk	The rating after taking account of the controls in place and how effective they are (section 12). Residual risk is compared with risk appetite.
Target risk	The rating expected once agreed treatment actions are complete. It must be within appetite, and has a date by which it will be reached.

Controls rated Ineffective give no reduction from inherent to residual risk. Controls rated Partly effective give a limited reduction, which the assessor must justify. Second line challenges any residual rating that is more than **[two]** levels below the inherent rating.

11.3 Response by residual rating

Residual rating	Required response	Who is told	Reassess at least
Critical	Outside appetite. Immediate action to reduce the risk; treatment plan agreed within [10 business days] ; interim controls in place.	CEO, CRO and Board Risk Committee [at once / at its next meeting]	[Monthly]
High	Usually outside appetite. Treatment plan agreed within [20 business days] , or formal risk acceptance under section 18.	Relevant executive and CRO; reported to the Board Risk Committee	[Quarterly]
Medium	Managed within the business. Treat where cost-effective; monitor KRIs.	Business unit head and second line	[Half-yearly]
Low	Accept and manage through routine controls.	Risk owner	[Annually]

The matrix rating is a common starting point. The Risk Appetite Statement decides what is inside or outside appetite for each risk category, and it can be stricter: for example, zero appetite for a breach of law or for customer harm means a Medium conduct risk may still require treatment. Financial risks such as capital adequacy and liquidity are also measured with their own metrics and limits (for example capital ratios and liquidity coverage) set in the Risk Appetite Statement.

12. Controls

A **control** is any measure that maintains or modifies risk (AS ISO 31000). CPS 220 para 19 requires a risk management framework that enables the entity to develop and implement strategies, policies, procedures and controls to manage material risks. CPS 230 requires internal controls designed and operating effectively (para 15(c)), designed, implemented and embedded in line with risk appetite (para 28), and regularly monitored, reviewed and tested (para 29). ASIC expects AFS licensees to establish controls designed to manage or mitigate risks and to fully implement and monitor them to ensure they are effective (RG 104.62).

12.1 Types of control

Type	Purpose	Examples
Preventive	Stop the risk event from happening	Segregation of duties, system access controls, approval limits, input validation, pre-employment screening
Detective	Find the risk event quickly when it happens	Reconciliations, exception reports, transaction monitoring, quality assurance checks, security monitoring
Corrective	Limit the impact and restore normal operation	Business continuity and disaster recovery plans, backups, incident response, customer remediation

Controls are also described as **automated** (performed by a system), **manual** or **IT-dependent manual**. Policies, training and committees support controls, but are not on their own evidence that a risk is controlled.

12.2 Key controls

A **key control** is a control that, on its own or with a small number of others, keeps a material risk within appetite, so that if it failed the residual risk would rise by at least one rating level or move outside appetite. Every Critical or High inherent risk must have identified key controls. Key controls are tested by second or third line at least **[annually]**, and the Board oversees the effectiveness of key internal controls in keeping operational risk within appetite (CPS 230 para 21(a)).

12.3 Design and operating effectiveness

Assessment	Question
Design effectiveness	If the control operates as intended, by the right person, at the right frequency, does it address the cause or consequence of the risk well enough to keep it within appetite?
Operating effectiveness	Has the control actually operated as designed, consistently, throughout the period, with evidence?

Control rating	Meaning
----------------	---------

Control rating	Meaning
Effective	Well designed and operating as intended, with evidence. Only minor improvements possible.
Partly effective	A design or operating weakness exists that reduces the control's ability to manage the risk, but the control still provides some protection. An issue must be raised.
Ineffective	The control is missing, poorly designed or not operating, and provides little or no protection. An issue must be raised and rated.

The overall control rating is the lower of the design and operating ratings. A control with an open issue against it is rated Partly effective or Ineffective until the issue is closed (RiskFA Incident & Issues Management Standard section 11.1). CPS 230 para 30 requires identified control gaps, weaknesses and failures to be included in the operational risk profile until they are remediated.

12.4 Control monitoring and testing

- **Control owner attestation** (first line): control owners confirm [quarterly] that their key controls operated, with evidence.
- **Control testing**: first line quality assurance, second line assurance reviews and Internal Audit test design and operating effectiveness. Testing frequency must be commensurate with the materiality of the risk (CPS 230 para 29); as a guide, key controls for Critical and High inherent risks are tested at least [annually], others at least every [2–3 years].
- **Test methods** include inquiry, observation, inspection of evidence, re-performance and automated or continuous testing of system data. Samples are sized to the frequency of the control.
- **Results** of testing are reported to senior management, and gaps or deficiencies are fixed in a timely manner (CPS 230 para 29), through issues under the RiskFA Incident & Issues Management Standard.
- **Triggers to reassess a control**: an incident or near miss, a KRI breach, a change to the process, system or service provider, an audit or regulator finding, or a change in the risk.

13. Risk and control self-assessment (RCSA)

The RCSA is how the first line regularly assesses its risks and controls, with second line challenge. It supports the comprehensive assessment of the operational risk profile required by CPS 230 para 26, and the identification and assessment of material risks and controls required by CPS 220 para 35(a) and SPS 220 para 22(b)(i).

1. **Scope:** each business unit and each critical operation, mapped to its processes, systems, service providers and obligations (CPS 230 para 26(b)).
2. **Assess:** risks are identified and rated (inherent and residual); controls are rated for design and operating effectiveness, using evidence such as testing results, incidents, issues, KRIs, complaints and audit findings.
3. **Challenge:** second line reviews and challenges ratings, especially any residual rating of Medium or below for a Critical or High inherent risk.
4. **Act:** issues and treatment actions are raised for weaknesses and risks outside appetite.
5. **Approve and report:** the business unit executive signs off the RCSA; results are reported to the Executive Risk Committee and summarised for the Board Risk Committee.

RCSAs are refreshed at least **[annually]**, and whenever a trigger occurs: a Critical or High incident, a material change to the business, process, system or service provider, a new product, or an audit or regulator finding.

14. Key risk indicators (KRIs)

A **key risk indicator** is a measure that gives early warning of a change in a risk's likelihood or consequence, or in the effectiveness of its controls. KRIs link day-to-day data to risk appetite.

- Each Level 1 risk category, each Critical or High residual risk and each critical operation has at least **[one]** KRI.
- Each KRI has an owner, a data source, a frequency and thresholds set in line with the Risk Appetite Statement.
- KRIs should look forward (for example staff turnover in a key team, unpatched critical vulnerabilities, overdue reconciliations) as well as backward (for example losses or incidents).
- Data used for KRIs must be accurate and timely. CPS 220 para 25 requires the management information system to be supported by a robust data framework, with prompt reporting of limit breaches.

KRI status	Meaning	Required response
Green: within appetite	The risk is at a level the Board accepts	Monitor
Amber: early warning trigger reached	The risk is approaching its tolerance limit	Risk owner tells the CRO within [5 business days] , records the cause and decides on action; second line challenges
Red: tolerance limit breached	The risk is outside appetite	Escalate as an appetite breach (section 9.1); action plan to return within appetite; recorded as an issue

15. Scenario analysis and stress testing

Scenario analysis and stress testing test whether the organisation could withstand severe events and whether its appetite, capital, liquidity and controls are adequate.

- APRA-regulated institutions must include forward-looking scenario analysis and stress testing programs, commensurate with size, business mix and complexity and based on severe but plausible assumptions (CPS 220 para 24).
- CPS 230 requires scenario analysis to identify and assess the potential impact of severe operational risk events, test operational resilience and identify the need for new or amended controls (para 26(c)), and a business continuity testing program that includes severe but plausible scenarios and an annual business continuity exercise (paras 42–43).
- ASIC expects fund operators to conduct stress testing and/or scenario analysis of liquidity risks at least annually, and to review the stress testing framework at least annually (RG 259.91–RG 259.92).
- **[Organisation]** runs at least **[annually]**: an enterprise scenario (for example a severe economic downturn combined with an operational event); scenarios for each material financial risk; operational risk scenarios for the top **[10]** operational risks (for example a cyber attack disabling a critical operation, failure of a material service provider, major fraud, or a large customer remediation); and, where relevant, climate scenarios (CPG 229).
- Results are reported to the Board Risk Committee, compared with appetite and capital, and used to update risk ratings, controls, business continuity plans and recovery and exit plans.

16. Emerging risks

An **emerging risk** is a new or changing risk whose likelihood, consequence or timing is uncertain and that could become material, such as new technology, new regulation, geopolitical change or a shift in customer behaviour.

- Second line runs an emerging risk scan at least **[half-yearly]**, using input from the business, industry bodies, regulators' publications, external research and incident data.
- Each emerging risk is recorded with an owner, a description of how it could affect **[Organisation]**, its expected timing and the signals to watch.
- Emerging risks are reported to the Executive Risk Committee and Board Risk Committee, and are moved into the risk register and rated once they can be assessed.

17. Change, new products and strategic decisions

- Strategic objectives and the business plan must be assessed for the material risks they create, and those risks managed through this Framework, including how changing the plans affects the risk profile (CPS 220 para 33; SPS 220 para 18).
- The impact of business and strategic decisions on the operational risk profile and operational resilience, including new products, services, geographies and technologies, must be assessed as part of planning (CPS 230 para 25).
- New products, material changes to products, systems or processes, new material service providers, outsourcing and acquisitions follow the **[New Product and Change Approval Policy]**: a risk assessment using this Framework, second line review and approval at the right level before launch.
- A material change to the size, business mix or complexity of operations triggers an assessment of whether this Framework needs to change (CPS 220 para 48; SPS 220 para 31).

18. Incidents, issues and risk acceptance

- Incidents, near misses and issues are identified, recorded, rated, escalated, notified, investigated and closed under the RiskFA Incident & Issues Management Standard, using the rating scale in this Framework. CPS 230 para 31 requires incidents and near misses to be taken into account in the assessment of the operational risk profile and control effectiveness in a timely manner.
- Every Critical or High incident and every issue is linked to the affected risks and controls, and the RCSA is updated.
- A risk outside appetite may be accepted only formally, by a person with the right authority, with reasons, interim controls and a review date of no more than **[12 months]**. Acceptances outside appetite need Board Risk Committee approval. A risk acceptance can never be used for a breach of law or for ongoing customer harm.

19. Risk culture

Risk culture is the shared values, beliefs and behaviours that shape how people identify, discuss and act on risk. The Board must form a view of the risk culture, and the extent to which it supports the organisation operating within its risk appetite, identify any desirable changes and ensure steps are taken to address them (CPS 220 para 9(b)). The Risk Management Strategy must outline how all persons are made aware of the framework and how an appropriate risk culture is instilled (CPS 220 para 30(e); SPS 220 para 22(f)). ASIC expects fund operators to foster a strong risk management culture (RG 259.37).

- **Tone and example:** the Board and executives talk about risk openly and act on bad news promptly.
- **Speaking up:** staff are encouraged to raise risks, incidents and concerns; honest mistakes reported promptly are treated as a chance to learn. The RiskFA Whistleblower Policy protects disclosures.
- **Accountability:** risk and control outcomes are part of performance and variable remuneration outcomes under the RiskFA Remuneration Policy (CPS 511 where it applies), and the RiskFA Consequence Management Framework.
- **Capability:** all staff complete risk management training at induction and **[annually]**; risk owners and control owners receive role-specific training.
- **Measurement:** risk culture is assessed at least every **[2 years]** using surveys, behavioural indicators (for example the share of issues self-identified by the business, overdue actions, late incident reporting, appetite breaches) and second and third line observations, and reported to the Board.

20. Risk reporting and the Board

The management information system must give the Board, Board committees and senior management regular, accurate and timely information on the risk profile, in normal conditions and in stress (CPS 220 paras 23(g), 25; SPS 220 para 16(f)). CPS 230 para 21(a) requires the Board to receive regular updates on the operational risk profile.

Report	Audience	Frequency	Content
Enterprise risk report	Board Risk Committee and Board	[Quarterly]	Risk profile against appetite; appetite and limit breaches; Critical and High risks and their trend; key control failures; KRIs at Amber or Red; significant incidents, issues and regulatory notifications; emerging risks; CRO's view
CRO's independent report	Board Risk Committee	[Quarterly] , plus at any time on a material matter	The CRO's own opinion on the risk profile, risk culture and the adequacy of the Framework, free of first line editing
Executive risk report	Executive Risk Committee	[Monthly]	As above, at greater detail, with business unit views and actions
Business unit risk report	Business unit leadership	[Monthly]	Risks, KRIs, control testing results, incidents, issues and overdue actions
Annual Framework report	Board Risk Committee and Board	[Annually]	Effectiveness of the Framework, results of the annual and comprehensive reviews, RCSA and control testing coverage, risk culture assessment, and the basis for the risk management declaration

Reports focus on insight, trends, customer impact and accountability, not volume. Bad news is reported promptly and never held until the next scheduled report.

21. Review, assurance and regulatory obligations

21.1 Reviews of this Framework

Requirement	CPS 220 (ADIs and insurers)	SPS 220 (RSE licensees)
Annual review	Compliance with, and effectiveness of, the framework reviewed by internal and/or external audit at least annually; results to the Board Audit Committee (para 44)	A review of the appropriateness, effectiveness and adequacy of the framework in each year without a comprehensive review (para 28); internal and external audit arrangements to ensure compliance with the framework (para 30)
Comprehensive review	Appropriateness, effectiveness and adequacy reviewed by operationally independent, appropriately trained and competent persons at least every three years; results to the Board Risk Committee (para 45). Scope in paras 46–47	Same, at least every three years (para 27). Scope in para 29, including the risk appetite statement, RMS, policies and procedures and internal control systems
Material change	Assess whether the framework needs amendment or review (para 48)	Same (para 31)
Operational risk	The required reviews must cover operational risk management as set out in CPS 230 para 15 (CPS 230 para 16)	Same (CPS 230 para 16)

AFS licensees should review their risk management systems at least annually (RG 259.28 for fund operators; RG 104 Table 3 asks whether risk management measures are reviewed annually). An independent comprehensive review at least every three years is good practice for fund operators (RG 259.55–RG 259.56) and for other licensees.

21.2 Risk management declaration

- **ADIs and insurers:** the Board makes an annual risk management declaration to APRA covering the matters in CPS 220 Attachment A, signed by the Board chair and the Board Risk Committee chair (para 49). It must be qualified if there has been a significant breach of, or material deviation from, the framework (para 50). It is submitted within four months of the annual balance date for an ADI or authorised banking NOHC that is not a disclosing entity and for a Level 3 Head, otherwise within three months (para 51).
- **RSE licensees:** the Board provides an annual risk management declaration signed by two directors covering SPS 220 Attachment A (para 32), on or before the day annual information is due under APRA's reporting standards (para 33). A qualified declaration describes any material deviation and the steps to remedy it (para 34).
- **[Organisation]** supports the declaration with: the annual Framework report; certifications from executives and accountable persons on risks and controls in their areas; the results of the annual and comprehensive reviews; and a list of significant breaches and material deviations.

21.3 Notifications to APRA about the Framework

Obligation	Applies to	When
Submit the Risk Appetite Statement, business plan and Risk Management Strategy on adoption and after any material revision (CPS 220 para 52)	ADIs and insurers	As soon as practicable and no more than 10 business days after Board approval
Significant breach of, or material deviation from, the risk management framework, or the framework did not adequately address a material risk (CPS 220 para 53; SPS 220 para 35)	ADIs, insurers, RSE licensees	Within 10 business days after becoming aware (CPS 220: as soon as practicable and no more than 10 business days)
Material or prospective material change to size, business mix and complexity (CPS 220 para 54; SPS 220 para 36)	ADIs, insurers, RSE licensees	CPS 220: as soon as practicable and no more than 10 business days ; SPS 220: as soon as practicable

Notifications about incidents, critical operations, information security, breaches of law and FAR events are covered in the RiskFA Incident & Issues Management Standard.

21.4 How CPS 220 and CPS 230 fit together

- CPS 220 (or SPS 220) sets the enterprise risk management framework for all material risks. CPS 230 sets specific requirements for operational risk, business continuity and service providers.
- Operational risk management must be developed and maintained **as part of** the risk management framework required under CPS 220 and SPS 220 (CPS 230 para 15) and integrated into the overall framework and processes (para 17). It is not a separate framework.
- CPS 230 applies to RSE licensees as well as ADIs and insurers (CPS 230 para 2(e)). The reissued CPS 230 (determination No. 1 of 2026) commenced on 1 July 2026 (para 6).
- This Framework provides the shared elements both standards rely on: governance, appetite, taxonomy, rating scale, controls, RCSA, KRIs, incidents and issues, and reporting. The RiskFA Operational Risk Management Policy, the RiskFA Business Continuity Policy and [\[Service Provider Management Policy\]](#) add the CPS 230 specifics.

22. Accountability and compliance with this Framework

- Every material risk has a named risk owner, and every key control a named control owner. For FAR accountable entities, the risk and control responsibilities of accountable persons are consistent with their accountability statements and the accountability map (FAR Act ss33–34).
- Breaches of this Framework (for example operating outside appetite without escalation, failing to record risks or incidents, or not testing key controls) are recorded as issues, reported to the CRO and managed under the RiskFA Consequence Management Framework.
- Exemptions from this Framework need the written approval of the CRO, are time-limited and are reported to the Board Risk Committee.

23. Related documents

- RiskFA Risk Appetite Statement
- RiskFA Incident & Issues Management Standard
- [\[Risk Management Strategy\]](#), [\[Business Plan\]](#), the RiskFA Operational Risk Management Policy, the RiskFA Compliance and Breach Reporting Policy, the RiskFA Cyber Security Policy, [\[Service Provider Management Policy\]](#), the RiskFA Business Continuity Policy, [\[New Product and Change Approval Policy\]](#)
- the RiskFA Whistleblower Policy, the RiskFA Remuneration Policy and the RiskFA Consequence Management Framework
- APRA: CPS 220 *Risk Management* and CPG 220 *Risk Management*; SPS 220 *Risk Management*; CPS 230 *Operational Risk Management* and CPG 230; CPS 234 *Information Security*; CPS 510 and SPS 510 *Governance*; SPS 515 *Strategic Planning and Member Outcomes*; CPS 511 *Remuneration*; CPG 229 *Climate Change Financial Risks*
- Legislation: *Financial Accountability Regime Act 2023*; *Corporations Act 2001* s912A
- ASIC: RG 104 *AFS licensing: Meeting the general obligations*; RG 259 *Risk management systems of fund operators*
- Standards: AS ISO 31000:2018 *Risk management — Guidelines*

Appendix A. Rating matrix

Read the rating where the likelihood row meets the consequence column. Likelihood is defined in Appendix C and consequence in Appendix B.

Likelihood ↓ / Consequence →	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Severe
5 Almost certain	Medium	High	High	Critical	Critical
4 Likely	Low	Medium	High	Critical	Critical
3 Possible	Low	Medium	High	High	Critical
2 Unlikely	Low	Low	Medium	High	High
1 Rare	Low	Low	Medium	Medium	High

The same 25 combinations, grouped by rating:

Rating	Count	Likelihood × consequence combinations
--------	-------	---------------------------------------

Rating	Count	Likelihood × consequence combinations
Critical	5	Almost certain × Major; Almost certain × Severe; Likely × Major; Likely × Severe; Possible × Severe
High	8	Almost certain × Minor; Almost certain × Moderate; Likely × Moderate; Possible × Moderate; Possible × Major; Unlikely × Major; Unlikely × Severe; Rare × Severe
Medium	6	Almost certain × Insignificant; Likely × Minor; Possible × Minor; Unlikely × Moderate; Rare × Moderate; Rare × Major
Low	6	Likely × Insignificant; Possible × Insignificant; Unlikely × Insignificant; Unlikely × Minor; Rare × Insignificant; Rare × Minor

- A Severe consequence is never rated below High, however unlikely: such risks need key controls and scenario testing.
- Do not change the matrix layout. Calibrate the thresholds in Appendices B and C instead, so that ratings stay comparable across the industry.

Appendix B. Consequence descriptors

Rate each impact category, then take the **highest**. Columns 5 to 2 are the same thresholds as Critical, High, Medium and Low in section 8 of the RiskFA Incident & Issues Management Standard.

Impact category	5 Severe (Critical)	4 Major (High)	3 Moderate (Medium)	2 Minor (Low)	1 Insignificant (Low)
Financial (loss, cost or remediation)	≥ [\$5m]	[\$1m] to < [\$5m]	[\$100k] to < [\$1m]	[\$10k] to < [\$100k]	< [\$10k]
Customers	Widespread harm, or serious harm to vulnerable customers	Many customers affected, or significant harm to some	Some customers affected; limited harm	Few or no customers affected; no lasting harm	No customer impact

Impact category	5 Severe (Critical)	4 Major (High)	3 Moderate (Medium)	2 Minor (Low)	1 Insignificant (Low)
Regulatory and legal	Significant breach; likely regulator action or licence impact	Breach that is reportable or likely to attract regulator attention	Breach of law or policy with limited consequences	Minor policy breach	No breach; minor process deviation
Operations and critical operations	Critical operation disrupted beyond tolerance	Critical operation disrupted within tolerance, or major disruption to other operations	Moderate disruption; workarounds in place	Minimal disruption	No noticeable disruption
Information security and privacy	Material information security incident (CPS 234) or large-scale eligible data breach	Eligible data breach, or security incident affecting sensitive systems	Contained security or privacy incident; no serious harm likely	Policy breach with no data exposed	Security event with no policy breach and no impact
Reputation	Sustained national media or public attention; loss of stakeholder confidence	Media or stakeholder attention	Limited external awareness	Internal only	No reputational impact

Set the dollar thresholds against your organisation's size, for example Severe at [1%] of annual net profit or [0.5%] of capital. The example values suit a mid-to-large entity; a smaller licensee, fund or insurer might use [\$500k] / [\$100k] / [\$10k] / [\$1k]. Keep the thresholds identical in this Framework and in the Incident & Issues Management Standard.

Appendix C. Likelihood scale

Rate the likelihood of the consequence you rated (not of any event at all) over the assessment period of [12 months]. Use the description, the frequency or the probability, whichever fits the information available.

Level	Description	Frequency (guide)	Probability in the next [12 months]
5 Almost certain	Expected to occur in most circumstances; has happened regularly here	[More than once a year]	[More than 90%]
4 Likely	Will probably occur; has happened here recently or often in the industry	[About once every 1–2 years]	[50% to 90%]
3 Possible	Might occur; has happened here before or occasionally in the industry	[About once every 2–10 years]	[10% to < 50%]
2 Unlikely	Could occur but not expected; has happened elsewhere in the industry	[About once every 10–100 years]	[1% to < 10%]
1 Rare	May occur only in exceptional circumstances	[Less than once every 100 years]	[Less than 1%]

For high-volume processes, likelihood can also be expressed per transaction or per customer (for example [1 in 10,000]). Whichever measure you use, apply it consistently and record the basis for the rating.

Appendix D. Glossary of core terms

Term	Meaning
Risk	The effect of uncertainty on objectives (AS ISO 31000). Described as a cause, an event and a consequence.
Material risk	A risk that could have a material impact, financial or non-financial, on the organisation or on the interests of depositors and/or policyholders (CPS 220 para 20) or beneficiaries (SPS 220 para 6).
Risk management framework	The totality of systems, structures, policies, processes and people that identify, measure, evaluate, monitor, report and control or mitigate material risks (CPS 220 para 20; SPS 220 para 6 uses similar wording). This document is its top level.
Risk appetite	The amount and type of risk the organisation is willing to accept in pursuit of its objectives, set by the Board.
Risk tolerance / limits	Measurable boundaries that put risk appetite into practice. For APRA-regulated entities, the maximum level of risk the entity is willing to operate within for each material risk, expressed as a risk limit (CPS 220 para 28(b); SPS 220 para 20(b)).
Early warning trigger	A KRI threshold, inside the tolerance limit, at which the risk owner must investigate and consider action.
Risk Management Strategy (RMS)	For APRA-regulated entities, the Board-approved document describing the strategy for managing each material risk and the key elements of the framework (CPS 220 para 30; SPS 220 para 22).
Risk owner	The named senior person accountable for managing a risk within appetite.
Control	A measure that maintains or modifies risk, for example a process, policy, device, practice or system check. Preventive, detective or corrective.
Key control	A control that on its own or with a few others keeps a material risk within appetite (section 12.2).
Control owner	The person accountable for designing, operating and evidencing a control.
Design effectiveness	Whether a control, operating as intended, would adequately manage the risk.

Term	Meaning
Operating effectiveness	Whether a control has actually operated as designed, consistently, over the period.
Control testing	Independent checking, with evidence, of a control's design and operating effectiveness.
Inherent risk	The risk rating before controls.
Residual risk	The risk rating after taking account of existing controls and their effectiveness.
Target risk	The risk rating expected after agreed treatment actions are complete.
Risk treatment	Action to modify a risk, for example by avoiding it, reducing its likelihood or consequence, sharing it or retaining it by informed decision (AS ISO 31000 clause 6.5).
Risk acceptance	A formal, time-limited decision by an authorised person to accept a risk or issue without further treatment (section 18).
Risk and control self-assessment (RCSA)	The first line's regular assessment of its risks and controls, challenged by second line (section 13).
Key risk indicator (KRI)	A measure that gives early warning of a change in a risk or in the effectiveness of its controls (section 14).
Scenario analysis	Assessing the impact of a specific severe but plausible event or combination of events.
Stress testing	Assessing the effect of severe but plausible changes in conditions on financial position, capital, liquidity or operations.
Emerging risk	A new or changing risk whose likelihood, consequence or timing is uncertain but that could become material (section 16).
Risk culture	The shared values, beliefs and behaviours that shape how people identify, discuss and act on risk.
Risk profile	The full set of risks the organisation faces, their ratings and their position against appetite.

Term	Meaning
Three lines of accountability	First line (business owns and manages risk), Second line (Risk and Compliance: frameworks, challenge, oversight), Third line (Internal Audit: independent assurance).
Accountable person	Under FAR, a person who, because of their position, has actual or effective senior executive responsibility for management or control of an accountable entity, or of a significant or substantial part or aspect of its operations or its relevant group, or who has a prescribed responsibility or holds a prescribed position (FAR Act s10).
Incident, Near miss, Issue, Breach, Root cause, Extent of condition, Action, Customer remediation, Critical operation, Material service provider, Reportable situation	As defined in the RiskFA Incident & Issues Management Standard.
Rating scale	Critical, High, Medium, Low, on the highest of six impact categories: Financial; Customers; Regulatory and legal; Operations and critical operations; Information security and privacy; Reputation (section 11 and Appendices A to C).

Appendix E. Document hierarchy

Level	Documents	Owner	Approval	Review
1. Framework and Board statements	Risk Management Framework; Risk Appetite Statement; [Risk Management Strategy] ; [Business Plan]	[CRO] ([CEO] for the business plan)	[Board] , on recommendation of the [Board Risk Committee]	At least [annually] ; business plan reviewed at least annually (CPS 220 para 32)
2. Policies	One per Level 1 risk category or major area, for example Operational Risk Management, Compliance, Information Security, Service Provider Management, Business Continuity, Credit, Liquidity, Investment, Conduct, Fraud, Privacy, AML/CTF	Relevant executive, with second line	[Board or Board Risk Committee]	At least every [2] years
3. Standards	Organisation-wide minimum requirements and methods, for example Incident & Issues Management Standard, Control Testing Standard, KRI Standard, Model Risk Standard	[CRO] or relevant second line head	[CRO / Executive Risk Committee]	At least every [2] years
4. Procedures and guidelines	Step-by-step instructions within a business unit or function	Business unit head	Business unit head, with second line review for key controls	At least every [2–3] years, or on change

Appendix F. Map to CPS 220 and SPS 220 requirements

Use this map to show where each minimum element of the risk management framework is met. Elements met outside this Framework are named in the right-hand column.

Requirement	CPS 220	SPS 220	Where it is met
Board responsibility for the framework	para 9	para 7	Sections 5–6
Material risks covered	para 26	paras 10–13	Section 8
Risk appetite statement	paras 23(a), 27–28	paras 16(a), 19–20	Section 9; RiskFA Risk Appetite Statement
Risk Management Strategy	paras 23(b), 29–30	paras 16(b), 21–22	This Framework and [Risk Management Strategy] (section 7)
Business plan and strategic risk	paras 23(c), 31–33	para 18 (and SPS 515)	[Business Plan] ; section 17
Policies and procedures for identifying and assessing risks and controls, mitigation and control testing, escalation, compliance, review	para 35	para 22(b)	Sections 10–14, 18; Level 2 and 3 documents
Roles, responsibilities and reporting structures	para 23(d)	para 16(e)	Sections 5–6
Designated, operationally independent risk management function	paras 23(e), 37	paras 16(c), 24	Section 5
CRO	paras 38–40	Not required by SPS 220	Section 6
Compliance function	para 43	Not specified in SPS 220	Sections 5–6
ICAAP	para 23(f)	Not applicable	[ICAAP document]
Management information system and data	paras 23(g), 25	para 16(f)	Sections 14, 20

Requirement	CPS 220	SPS 220	Where it is met
Scenario analysis and stress testing	para 24	Not specified in SPS 220 (see CPS 230 para 26(c))	Section 15
Review process: annual and comprehensive	paras 23(h), 44–48	paras 16(g), 27–31	Section 21.1
Risk culture and awareness	paras 9(b), 30(e)	para 22(f)	Section 19
Risk management declaration	paras 49–51, Attachment A	paras 32–34, Attachment A	Section 21.2
Notifications to APRA	paras 52–55	paras 35–36	Section 21.3



[Risk Taxonomy](#)
[Operations](#)
[Library](#)
[Obligations Register](#)
[Why a standard](#)
[About](#)

Disclaimer

© 2026 Risk Frameworks Australia

Free general information only, provided free of charge. Not legal, financial or other professional advice, and used at your own risk. [Read the full disclaimer.](#)