

Risk Appetite Statement

A ready-to-adopt Risk Appetite Statement the Board can approve: how much risk the organisation will accept, the measurable tolerances that put it into practice, and what happens when a tolerance is breached.

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

How to use this industry statement. Adopt the structure, appetite scale, terms and green/amber/red trigger levels as written, so that your organisation speaks the same language as the rest of the industry. Choose the appetite level for each risk category, replace the example metrics and the text in **[square brackets]** with your own measures and thresholds, delete risk categories that are not material to you (for example insurance risk if you are not an insurer), and have the Board approve the Statement. Every metric and threshold in this template is an **example only**: set your own from your strategy, risk profile and capital and liquidity strength. 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 Appetite Statement
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] , aligned with the business planning cycle, and after any material change in strategy, risk profile, capital or liquidity position, regulation or the external environment
Parent framework	the RiskFA Risk Management Framework
Copy to APRA	Within 10 business days of Board approval of a new or materially revised Statement (APRA-regulated institutions under CPS 220 para 52)

1. Purpose

This Statement sets out the amount and type of risk the Board of [Organisation] is willing to accept in pursuit of its strategic objectives and business plan, having regard to the interests of [customers / depositors / policyholders / members] . It:

- states the Board's overall risk appetite and its appetite for each material risk;
- sets measurable **risk tolerances** (limits) and earlier **trigger levels** for each material risk, so that appetite can be monitored in practice;
- names the matters for which [Organisation] has **zero tolerance**;
- sets out what must happen when a trigger or tolerance is reached or breached; and
- sets out how the Statement is monitored, reported, reviewed and approved.

The Statement is a core part of [Organisation]'s the RiskFA Risk Management Framework. It guides strategy, business planning, product decisions, limits, delegations, control design and remuneration outcomes. Decisions that would take [Organisation] outside appetite need prior Board approval.

2. Scope and regulatory basis

This Statement applies to [Organisation] and [its subsidiaries / the group], all business units, products and services, and activities performed for us by service providers.

Where they apply, it is designed to meet the following requirements (as at October 2026).

Delete those that do not apply to you.

Requirement	Source	Where addressed
The Board sets the risk appetite within which it expects management to operate, and approves the risk appetite statement and risk management strategy. The Board forms a view of whether risk culture supports operating within risk appetite.	CPS 220 para 9(a)-(b)	Sections 7, 19
The risk management framework includes a risk appetite statement.	CPS 220 para 23(a); SPS 220 para 16(a)	Whole Statement
Maintain an appropriate, clear and concise risk appetite statement that addresses all material risks, approved by the Board. Material risks include at least credit, market and investment, liquidity, insurance, operational and strategic risks, and other material risks.	CPS 220 paras 26-27	Sections 7, 9-12
The statement must at a minimum convey: (a) risk appetite; (b) for each material risk, a risk tolerance expressed as a risk limit based on appetite, risk profile and capital strength; (c) the process for setting tolerances at an appropriate level, based on the impact if breached and the likelihood the risk is realised; (d) the process for monitoring compliance with each tolerance and acting on a breach; (e) the timing and process for review.	CPS 220 para 28(a)-(e)	(a) sections 6-7; (b) sections 9-12; (c) section 14; (d) sections 16-17; (e) section 18

Requirement	Source	Where addressed
RSE licensees: maintain an up-to-date risk appetite statement covering business operations and each category of material risk, approved by the Board, with the same five minimum elements, considering the interests of beneficiaries. Tolerances are, where possible, a measurable limit on the risk remaining after taking account of mitigants.	SPS 220 paras 10, 19, 20(a)-(e)	Sections 7, 9-14, 16-18
Submit a copy of the risk appetite statement to APRA on adoption and after any material revision, within 10 business days of Board approval.	CPS 220 para 52	Section 18
Notify APRA within 10 business days of becoming aware of a significant breach of, or material deviation from, the risk management framework, or that the framework did not adequately address a material risk.	CPS 220 para 53; SPS 220 para 35	Section 17
Operational risk: an assessment of the operational risk profile with a defined risk appetite supported by indicators, limits and tolerance levels; internal controls designed and operating effectively. The Board oversees the effectiveness of key internal controls in keeping the operational risk profile within risk appetite.	CPS 230 paras 15(b)-(c), 21(a)	Sections 4, 11
Design, implement and embed internal controls to mitigate operational risks in line with risk appetite; regularly monitor, review and test controls for design and operating effectiveness.	CPS 230 paras 28-29	Sections 4, 11
For each critical operation, set tolerance levels for maximum disruption time, maximum data loss and minimum service levels. The Board approves the tolerance levels. Failure to meet a tolerance level is reported to the Board with a remediation plan; disruption to a critical operation outside tolerance is notified to APRA within 24 hours.	CPS 230 paras 21(b), 37, 40, 41	Sections 11.2, 17

APRA's guidance in CPG 220 *Risk Management* (April 2018, paras 46-59) explains APRA's view of good practice for risk appetite statements, and CPG 229 *Climate Change Financial Risks* (November 2021) covers climate risk in risk appetite. Guidance is not a legal requirement. Non-APRA-regulated licensees (for example AFS and credit licensees) have no specific requirement to hold a risk appetite statement, but a Board-approved statement is good practice and supports the general obligation to have adequate risk management systems (*Corporations Act 2001* s912A(1)(h), where it applies).

3. Key definitions

Term	Meaning
Risk	The effect of uncertainty on objectives (AS ISO 31000).
Material risk	A risk that could have a material impact, financial or non-financial, on [Organisation] or on the interests of [customers / depositors / policyholders / members] (CPS 220 para 20 wording; SPS 220 para 6).
Risk capacity	The maximum level of risk [Organisation] can take before breaching regulatory capital or liquidity requirements, its operational capability or its obligations to customers and other stakeholders (FSB 2013 definition, adapted).
Risk appetite	The amount and type of risk [Organisation] is willing to accept in pursuit of its objectives, set by the Board. It sits inside risk capacity.
Risk tolerance / limit	A measurable boundary that puts appetite into practice: the maximum level of a material risk [Organisation] is willing to operate within. Exceeding it is a Red status (outside appetite).
Trigger level	An earlier warning threshold set inside the tolerance. Reaching it is an Amber status and prompts action before the tolerance is breached. CPG 220 para 57 describes key indicators with thresholds around the tolerance.
Risk profile	The current level of risk [Organisation] is exposed to, before and after controls, at a point in time.
Key risk indicator (KRI)	A metric that tracks the level of a risk, or the effectiveness of the controls over it, against trigger and tolerance levels.
Control	A measure that maintains or modifies risk (AS ISO 31000). Controls are preventive (stop the event), detective (find it quickly) or corrective (limit and fix the impact). Key controls are those the organisation relies on most to keep a material risk within appetite.
Control effectiveness	Whether a control is designed to address the risk (design effectiveness) and works as intended, consistently, over time (operating effectiveness), as shown by control testing (CPS 230 para 29).
Zero tolerance	A matter the Board will not accept in any circumstances. Any occurrence is outside appetite and must be escalated immediately (section 13).

Term	Meaning
Critical operation, Incident, Issue, Breach	As defined in the RiskFA Incident & Issues Management Standard.

4. How risk appetite and controls work together

Risk appetite + effective controls = management of risk. The Board decides how much risk to accept. Management keeps the risk profile within that appetite through controls that are well designed, operate effectively and are tested. Everything else in the framework, including ratings, registers, indicators and reports, is how [Organisation] records and communicates whether that is working.

1. **Set appetite.** The Board sets the appetite level and tolerances for each material risk (sections 6-12).
2. **Design and embed controls.** Risk owners and control owners design, implement and embed preventive, detective and corrective controls that keep each risk within appetite (risk treatment under AS ISO 31000; CPS 230 para 28).
3. **Test controls.** Key controls are tested for design and operating effectiveness, at a frequency matched to the materiality of the risk (CPS 230 para 29). A key control rated ineffective is an issue under the RiskFA Incident & Issues Management Standard.
4. **Monitor the risk profile.** KRIs are measured against trigger levels and tolerances (sections 9-12, 16).
5. **Act and escalate.** When a trigger is reached or a tolerance breached, controls are strengthened, the risk is reduced or the Board decides on the risk (section 17).
6. **Review.** Appetite, tolerances and controls are reviewed as the business, risks and environment change (section 18).

A risk can only be said to be **within appetite** if both the KRIs are within tolerance **and** the key controls over it are effective. A risk with green KRIs but ineffective key controls is reported as **Amber** until the controls are fixed.

5. Principles

1. **The Board owns appetite.** The Board sets and approves risk appetite and holds management to account for operating within it.
2. **Appetite links to strategy.** Appetite is set alongside the strategy and business plan, and within risk capacity, with a buffer below capacity.
3. **Every material risk is covered.** Every material risk has a qualitative statement, an appetite level, at least one measurable tolerance where possible, and a named risk owner. Where a quantitative tolerance is not possible, the qualitative tolerance is written clearly enough to tell when it has been exceeded (CPG 220 paras 47, 58).
4. **Customers come first.** Appetite considers the interests of [customers / depositors / policyholders / members], not just financial outcomes.
5. **Early warning, not surprise.** Trigger levels give time to act before a tolerance is breached.
6. **Breaches are escalated, not hidden.** Breaches are reported promptly and honestly; a breach is never resolved by quietly changing the limit.
7. **Clear and concise.** The Statement is written so that staff can understand what it means for their decisions (CPS 220 para 27; CPG 220 para 50).
8. **Proportionate.** Measures and reporting match the size, business mix and complexity of [Organisation].

6. The risk appetite scale

[Organisation] uses one five-level scale for every risk category. Each category is given one level in section 9.

Level	Meaning in plain words	Typical use
Averse	Avoid the risk wherever possible. Accept only the minimum that cannot reasonably be avoided, and act immediately if it arises.	Breaches of law, financial crime, unfair customer outcomes, serious harm to people
Minimal	Accept only very low levels of risk, where the controls are strong and the potential impact is small.	Liquidity, cyber security, critical operations, privacy
Cautious	Accept some risk where it is needed to deliver the strategy, with a preference for safe options and strong controls.	Credit, insurance underwriting, third party, data

Level	Meaning in plain words	Typical use
Open	Willing to consider all options and accept a moderate level of risk for a clear benefit, with controls matched to the risk.	Strategic growth, investment, innovation
Receptive	Willing to accept higher risk in pursuit of significant reward or long-term benefit, accepting a greater chance of loss or setback, within risk capacity.	Selected new ventures or pilots, limited in size by tolerance

The scale describes attitude to risk, not the amount of risk currently held. A Receptive appetite is still bounded by tolerances and by risk capacity. For zero-tolerance matters see section 13: they sit below Averse.

7. Overall risk appetite statement

The Board approves the following overall statement. Replace the example wording with your own.

[Organisation] overall risk appetite (example). [Organisation] exists to [purpose]. In pursuing its strategy, [Organisation] accepts the risks needed to [deliver value to customers / members and a sustainable return], provided that it: (1) always maintains capital above [Board capital target, e.g. regulatory minimum plus a management buffer] and liquidity above [Board liquidity target], including under severe but plausible stress; (2) treats customers fairly and does not accept outcomes that cause them avoidable harm; (3) complies with the law and its licence conditions; (4) keeps critical operations within the tolerance levels the Board has approved; (5) protects customer and organisational information; and (6) protects its reputation and the trust of [customers, members, regulators and the community]. [Organisation] has an overall **[Cautious]** appetite for risk, with a **Minimal** or **Averse** appetite for risks that threaten its financial soundness, customers, critical operations or compliance with the law.

8. Capacity, appetite, tolerance and triggers

Each material risk is managed in layers. Trigger levels and tolerances are set inside risk capacity, with a buffer.

Layer	Set by	Status	What it means
-------	--------	--------	---------------

Layer	Set by	Status	What it means
Risk capacity	Regulatory requirements, financial resources, operational capability	Beyond capacity	The organisation's viability or regulatory standing is at risk. Recovery or crisis plans apply.
Risk tolerance (limit)	Board	Red: outside appetite	The limit has been exceeded. Escalation to the Board Risk Committee and a plan to return within tolerance are required (section 17).
Trigger level	Board, or management where delegated	Amber: approaching tolerance	Early warning. The risk owner must act to bring the risk back to Green or explain why the trend will reverse.
Target range	Management, within Board appetite	Green: within appetite	Normal operations. Monitor and report as usual.

Where a metric works in the other direction (higher is better, for example a capital or liquidity ratio), the trigger level is set above the tolerance. Each metric in the register (Appendix A) records which direction applies.

9. Appetite by risk category: summary

The risk categories follow the RiskFA Risk Management Framework taxonomy. Technology and critical operations, cyber and information security, AI, third party and data and privacy are Level 2 risk types within Operational risk, shown separately because each has its own appetite. RSE licensees also add the Governance category (governance and investment governance risk, SPS 220 para 12(a)-(b)). The appetite levels below are **examples**: the Board sets its own.

Risk category	Example appetite level	Risk owner
Strategic (incl. capital)	[Open]	[CEO]
Credit	[Cautious]	[Chief Credit Officer]

Risk category	Example appetite level	Risk owner
Market and investment	[Cautious]	[Chief Financial Officer / Chief Investment Officer]
Liquidity	[Minimal]	[Chief Financial Officer / Treasurer]
Insurance	[Cautious]	[Chief Underwriting Officer / Appointed Actuary support]
Operational (general)	[Cautious]	[Chief Operating Officer]
Technology and critical operations	[Minimal]	[Chief Technology Officer]
Cyber and information security	[Minimal]	[Chief Information Security Officer]
Artificial intelligence (AI)	[Cautious]	[Accountable executive for AI]
Third party (incl. material service providers)	[Cautious]	[Chief Operating Officer]
Data and privacy	[Minimal]	[Chief Data Officer / Privacy Officer]
Compliance and regulatory	[Averse]	[Head of Compliance / General Counsel]
Conduct	[Averse]	[Accountable executive for customers]
Reputational	[Minimal]	[CEO]
Climate and sustainability	[Cautious]	[Chief Risk Officer / Chief Sustainability Officer]

About the example metrics in sections 10-12. Every metric, threshold and trigger level in the tables is an **example**, not a recommendation or a regulatory requirement. Replace them with measures that fit your business, and calibrate them using section 14. Where a metric names a prudential measure (for example the Liquidity Coverage Ratio), the regulatory minimum is set by the relevant APRA prudential standard; your tolerance should sit above it. Green is within appetite, Amber is the trigger level, Red is outside tolerance.

10. Financial risks

10.1 Strategic risk (including capital)

Statement. [Organisation] has an [Open] appetite for strategic risk where initiatives support its purpose and long-term sustainability, are within its capability to deliver, and keep capital above the Board's target in normal and stressed conditions. It has a [Minimal] appetite for capital falling below the Board's target buffer, and does not accept strategies that rely on falling below regulatory capital requirements.

Example metric	Green	Amber (trigger)	Red (tolerance)
Capital ratio (e.g. CET1 for ADIs, PCA coverage for insurers, ORFR target for RSE licensees) against Board target	$\geq$ [target + 1.0%]	[target] to < [target + 1.0%]	< [target]
Net profit after tax against plan	Within [10%] of plan	[10-20%] below plan	> [20%] below plan
Revenue from a single product, channel or client	$\leq$ [30%]	> [30%] to [40%]	> [40%]
Major strategic initiatives on time and on budget	$\geq$ [80%]	[60-80%]	< [60%]

10.2 Credit risk

Statement. [Organisation] has a [Cautious] appetite for credit risk. It lends [or invests] only where it understands the borrower or counterparty and is reasonably confident of repayment, and it avoids concentrations that could threaten its capital. It does not accept lending that is unsuitable for the customer.

Example metric	Green	Amber (trigger)	Red (tolerance)
----------------	-------	-----------------	-----------------

Example metric	Green	Amber (trigger)	Red (tolerance)
Loans 90+ days in arrears, % of portfolio	< [1.0%]	[1.0-1.5%]	> [1.5%]
Largest single counterparty exposure, % of capital	< [10%]	[10-20%]	> [20%] (and within any regulatory large exposure limit)
Largest industry concentration, % of portfolio	< [15%]	[15-20%]	> [20%]
New lending outside credit policy (exceptions), % of approvals	< [3%]	[3-5%]	> [5%]

10.3 Market and investment risk

Statement. [Organisation] has a [Cautious] appetite for market risk, including interest rate risk in the banking book and foreign exchange risk, and does not trade for speculative purposes [delete if you have a trading book]. For investment risk taken on behalf of [members / policyholders], [Organisation] accepts the level of investment risk set by each [investment option's] objectives and strategic asset allocation, and has a [Minimal] appetite for departing from them.

Example metric	Green	Amber (trigger)	Red (tolerance)
Interest rate risk in the banking book: change in economic value for a [200bp] shock, % of capital	< [5%]	[5-8%]	> [8%]
Trading Value at Risk against limit [if applicable]	< [80%] of limit	[80-100%] of limit	> limit
Unhedged foreign exchange exposure, % of capital	< [2%]	[2-3%]	> [3%]
Investment option asset allocation outside approved ranges	None	Any option within [1%] of a range limit	Any option outside its range for > [5 business days]

10.4 Liquidity risk

Statement. [Organisation] has a [Minimal] appetite for liquidity risk. It must always be able to meet its obligations as they fall due, including in severe but plausible stress, and holds liquid assets and diverse funding well above regulatory minimums. [RSE licensees: it must always be able to pay benefits, process switches and rollovers, and meet other member and fund obligations.]

Example metric	Green	Amber (trigger)	Red (tolerance)
Liquidity Coverage Ratio (ADIs subject to LCR)	$\geq$ [130%]	[115-130%]	$<$ [115%]
Net Stable Funding Ratio (ADIs subject to NSFR)	$\geq$ [115%]	[105-115%]	$<$ [105%]
Survival horizon under internal stress scenario	$\geq$ [90 days]	[60-90 days]	$<$ [60 days]
Funding from top [10] depositors or funders, % of total	$<$ [10%]	[10-15%]	$>$ [15%]
Liquid assets for each [investment option] under stress (RSE licensees)	$\geq$ [x times] stressed outflows	[1.5x-x]	$<$ [1.5x]

10.5 Insurance risk

Statement. [Organisation] has a [Cautious] appetite for insurance risk. It underwrites risks it understands and can price, reserves prudently, and uses reinsurance to limit the impact of large or catastrophe events on its capital. [Delete this section if you are not an insurer.]

Example metric	Green	Amber (trigger)	Red (tolerance)
Net loss ratio against plan	Within [5 points] of plan	[5-10 points] above plan	$>$ [10 points] above plan
Net retained catastrophe loss at [1-in-200 year] event, % of capital	$<$ [x%]	[x-y%]	$>$ [y%]
Outstanding claims reserves held at the Board's target probability of adequacy	$\geq$ [target]	Within [2 points] below target	$>$ [2 points] below target

Example metric	Green	Amber (trigger)	Red (tolerance)
Business written outside underwriting authority	[0]	Any instance	More than [x] in a quarter, or any above [\$X]

11. Operational risks

Under CPS 230 para 15(b), the operational risk appetite is supported by indicators, limits and tolerance levels; under para 21(a) the Board oversees the effectiveness of key internal controls in keeping the operational risk profile within appetite.

11.1 Operational risk (general)

Statement. [Organisation] has a [Cautious] appetite for operational risk. It accepts that some operational losses and errors will occur, but expects them to be small, found quickly and fixed at the root cause. It relies on key controls that are designed and operating effectively and are tested regularly.

Example metric	Green	Amber (trigger)	Red (tolerance)
Net operational losses in the quarter	< [\$250k]	[\$250k-\$1m]	> [\$1m]
Critical or High incidents in the quarter (RiskFA rating scale)	[0] Critical; ≤ [2] High	≤ [4] High	Any Critical, or > [4] High
Key controls rated effective in testing (design and operating)	≥ [95%]	[90-95%]	< [90%]
High or Critical actions overdue	[0]	Any overdue ≤ [30 days]	Any overdue > [30 days]

11.2 Technology and critical operations

Statement. [Organisation] has a [Minimal] appetite for disruption to its critical operations and the technology that supports them. It will not operate a critical operation outside the tolerance levels the Board has approved under CPS 230 para 37, and invests to keep critical systems supported, resilient and recoverable.

Example metric	Green	Amber (trigger)	Red (tolerance)
----------------	-------	-----------------	-----------------

Example metric	Green	Amber (trigger)	Red (tolerance)
Disruption to a critical operation against its tolerance level for the maximum period of disruption (CPS 230 para 37(a))	No disruption, or recovered in < [50%] of tolerance	Recovered in [50-100%] of tolerance	Disruption beyond tolerance (also notify APRA within 24 hours: CPS 230 para 41)
Data loss in a disruption against maximum data loss tolerance	Nil	Within tolerance	Beyond tolerance
Availability of systems supporting critical operations	≥ [99.9%]	[99.5-99.9%]	< [99.5%]
Business continuity plan tests completed and passed on schedule	[100%]	[90-100%]	< [90%], or any failed test not remediated within [90 days]
Unsupported (end-of-life) systems supporting critical operations	[0]	Any with an approved replacement plan	Any without an approved plan

The tolerance levels for each critical operation (maximum period of disruption, maximum data loss and minimum service levels) are approved by the Board and recorded in the register of critical operations in the RiskFA Business Continuity Policy (CPS 230 paras 21(b), 37, 39(a)). This Statement refers to them rather than repeating them.

11.3 Cyber and information security risk

Statement. [Organisation] has a [Minimal] appetite for cyber and information security risk. It protects the confidentiality, integrity and availability of its information assets in line with their criticality and sensitivity, and has no appetite for known critical vulnerabilities left unaddressed on internet-facing or critical systems.

Example metric	Green	Amber (trigger)	Red (tolerance)
Critical vulnerabilities on internet-facing systems patched or mitigated within [48 hours]	[100%]	[95-100%]	< [95%]

Example metric	Green	Amber (trigger)	Red (tolerance)
Privileged and remote access protected by phishing-resistant multi-factor authentication	[100%]	[98-100%]	< [98%]
Material information security incidents (CPS 234)	[0]	Any contained incident with no material impact	Any material incident
Information security control tests completed on schedule, with no unremediated material weakness	[100%]	Any test overdue ≤ [30 days]	Any material weakness not remediated on time (CPS 234 para 36 may apply)

11.4 Artificial intelligence (AI) risk

Statement. [Organisation] has a [Cautious] appetite for using AI. It supports AI that improves outcomes for customers and efficiency, where the use is recorded, risk-assessed before use, explainable to the level the decision needs, monitored, and subject to human oversight proportionate to the impact on customers. It has an **Averse** appetite for AI that makes or materially influences decisions about customers without appropriate human oversight, or that uses data in ways customers would not reasonably expect.

Example metric	Green	Amber (trigger)	Red (tolerance)
AI use cases recorded in the AI inventory and risk-assessed before use	[100%]	[95-100%]	< [95%], or any high-impact use case not assessed
High-impact AI use cases without documented human oversight	[0]	Any with oversight being put in place within [30 days]	Any in use without oversight
AI models outside performance or fairness thresholds	[0]	Any within [30 days] of detection with an action plan	Any unremediated > [30 days]

Example metric	Green	Amber (trigger)	Red (tolerance)
Complaints relating to automated or AI-assisted decisions	< [x] per quarter	[x-y]	> [y], or any systemic issue

As at October 2026 there is no AI-specific prudential standard. AI risk is managed under existing obligations (for example CPS 220, CPS 230, CPS 234, the *Privacy Act 1988* and the general conduct obligations). AS ISO/IEC 42001 *Information technology - Artificial intelligence - Management system* is a recognised standard you may use. The appetite above is good practice.

11.5 Third party risk (including material service providers)

Statement. [Organisation] has a [Cautious] appetite for third party risk. It uses service providers where they deliver better outcomes, but it remains accountable for the services they perform. It does not rely on a service provider unless it can continue to meet its obligations and manage the risks (CPS 230 para 14), and has a [Minimal] appetite for material service providers without a current risk assessment and tested exit or contingency arrangements.

Example metric	Green	Amber (trigger)	Red (tolerance)
Material service providers with a current risk assessment and due diligence	[100%]	[95-100%]	< [95%]
Material service providers with tested exit or contingency plans	[100%]	[90-100%]	< [90%]
Material service provider incidents breaching agreed service levels in the quarter	≤ [1]	[2-3]	> [3], or any affecting a critical operation beyond tolerance
Critical operations dependent on a single provider with no alternative	[0]	Any with an approved mitigation plan	Any without a plan

11.6 Data and privacy risk

Statement. [Organisation] has a [Minimal] appetite for data and privacy risk. It collects, uses, keeps and shares personal and business data only for clear purposes, keeps critical data accurate and complete, and protects it from loss or misuse.

Example metric	Green	Amber (trigger)	Red (tolerance)
Data quality score for critical data elements	≥ [98%]	[95-98%]	< [95%]
Eligible data breaches notified to the OAIC	[0]	Any suspected breach under assessment	Any eligible data breach
User access reviews completed on schedule for systems holding personal information	[100%]	[95-100%]	< [95%]
Personal information held beyond its retention period	[0] known instances	Disposal plan in place	No plan, or held > [12 months] beyond retention

12. Compliance, conduct, reputational and climate risks

12.1 Compliance and regulatory risk

Statement. [Organisation] has an [Averse] appetite for compliance and regulatory risk. It complies with the law, its licence conditions, prudential and regulatory requirements and its own policies. It accepts that breaches may occasionally occur despite effective controls; when they do, they must be identified, reported to regulators on time where required, and fixed at the root cause. Deliberate breaches are zero tolerance (section 13).

Example metric	Green	Amber (trigger)	Red (tolerance)
Regulatory notifications (reportable situations, APRA notifications, AUSTRAC reports) lodged late	[0]	-	Any late notification
Breach reportability decisions not made by day [20] after identification	[0]	Any between day [20] and [25]	Any after day [25]

Example metric	Green	Amber (trigger)	Red (tolerance)
Regulator findings or commitments overdue	[0]	Any overdue $\leq$ [30 days] with regulator informed	Any overdue $>$ [30 days]
Compliance obligations register attestations completed	[100%]	[95-100%]	$<$ [95%]

12.2 Conduct and customer risk

Statement. [Organisation] has an [Averse] appetite for conduct that causes unfair outcomes for customers. It designs and distributes products that meet the needs of their target market, communicates clearly, treats vulnerable customers with care, handles complaints fairly and promptly, and remediates affected customers quickly and fully. Knowingly causing unfair customer outcomes is zero tolerance (section 13).

Example metric	Green	Amber (trigger)	Red (tolerance)
Complaints per [1,000] customers	$<$ [x]	[x-y], or rising for [2] quarters	$>$ [y]
Complaints resolved within the RG 271 maximum timeframes	$\geq$ [98%]	[95-98%]	$<$ [95%]
Significant dealings inconsistent with a target market determination	[0]	Any under assessment	Any significant dealing (notify ASIC within 10 business days)
Customer remediation programs open more than [12 months]	[0]	Any with an approved plan and on track	Any off track
AFCA determinations against [Organisation] in the quarter	$\leq$ [x]	[x-y]	$>$ [y], or any systemic issue identified

12.3 Reputational risk

Statement. [Organisation] has a [Minimal] appetite for actions or associations that could damage the trust of customers, members, regulators, employees and the community. Reputational risk usually follows from other risks, so it is managed mainly by keeping those risks within appetite and by considering reputation in every significant decision.

Example metric	Green	Amber (trigger)	Red (tolerance)
Customer trust or satisfaction score (e.g. Net Promoter Score) against target	$\geq$ [target]	Within [5 points] below target	$>$ [5 points] below target
Negative national media coverage attributable to [Organisation]	None	Isolated coverage	Sustained coverage over [x] days
Escalated stakeholder or regulator concerns about [Organisation]'s conduct	[0]	[1]	$>$ [1], or any formal regulator action

12.4 Climate risk

Statement. [Organisation] has a [Cautious] appetite for climate-related financial risk (physical, transition and liability risk). It considers climate risk in its strategy, credit, investment, underwriting and operational decisions, and manages it within its existing risk appetite, as CPG 229 explains. It supports an orderly transition and has a [Minimal] appetite for new concentrations in assets or customers at high physical or transition risk without a mitigation plan.

Example metric	Green	Amber (trigger)	Red (tolerance)
Exposure to sectors at high transition risk, % of [lending / investments / premium]	$<$ [x%]	[x-y%]	$>$ [y%]
Exposure to locations at high physical risk (e.g. flood, bushfire), % of portfolio	$<$ [x%]	[x-y%]	$>$ [y%]
Progress against the Board's climate or emissions targets	On track	Behind by $\leq$ [10%]	Behind by $>$ [10%]

Example metric	Green	Amber (trigger)	Red (tolerance)
Climate scenario analysis completed and reported to the Board	Within [12 months]	[12-15 months]	> [15 months]

Entities required to report under the mandatory climate-related financial disclosure regime should check that the metrics here are consistent with what they disclose. Climate appetite above is good practice; CPG 229 is guidance, not a legal requirement.

13. Zero-tolerance matters

The Board has **zero tolerance** for the matters below. Zero tolerance means [Organisation] will **never knowingly accept** these, will not trade them off against profit or growth, and will act immediately when one is found. It does not mean they can never happen: controls reduce the chance but cannot remove it. What zero tolerance requires is that every occurrence, or reasonable suspicion of one, is escalated at once, investigated, reported to regulators where required, and dealt with under the RiskFA Consequence Management Framework.

- **Deliberate or knowing breach of the law**, licence conditions or prudential requirements, including continuing an activity after becoming aware that it breaches the law.
- **Internal fraud, bribery and corruption** by employees, directors, contractors or service providers acting for [Organisation].
- **Knowingly facilitating money laundering, terrorism financing or sanctions breaches.**
- **Knowingly causing unfair outcomes for customers**, including selling a product we know is unsuitable for the customer, charging fees for no service, or delaying remediation we know is owed.
- **Concealing or misreporting** incidents, breaches, losses or risk information, or misleading the Board, auditors or regulators.
- **Deliberately bypassing or overriding key controls** without approved authority.
- **Retaliation against whistleblowers** or anyone who raises a concern in good faith.
- **Knowingly exposing people to serious risk to their health and safety.**

Honest mistakes that are promptly reported are not zero-tolerance matters. They are managed as incidents under the RiskFA Incident & Issues Management Standard. The aim is to encourage speaking up, not to discourage reporting.

14. Setting and calibrating tolerances

Tolerances must be set at an appropriate level, based on an estimate of the impact if the tolerance is breached and the likelihood that each material risk is realised (CPS 220 para 28(c); SPS 220 para 20(c)). For each metric the risk owner, with second line challenge:

1. identifies the material risk and the outcome the Board wants to avoid;
2. chooses metrics that show the level of the risk or the effectiveness of the key controls, preferring forward-looking (leading) indicators where possible;
3. sets the **tolerance** from the impact if breached (using the RiskFA rating scale: Critical, High, Medium, Low), risk capacity, capital and liquidity strength and the business plan, so that a Red breach would not exceed the Board's appetite;
4. sets the **trigger level** far enough inside the tolerance to allow time to act, considering how quickly the metric can move;
5. tests the levels against historical data and stress scenarios, and confirms the data source is reliable;
6. records the metric in the register (Appendix A) with owner, data source, frequency and direction; and
7. submits new or changed Board-level tolerances to the [Board Risk Committee] for recommendation to the Board.

Where a quantitative tolerance is not possible, a qualitative tolerance is written clearly enough to tell when it has been exceeded (CPG 220 para 58). Tolerances are never loosened to resolve a current breach without Board approval and a recorded reason.

15. Putting appetite into practice

- **Cascading.** Board tolerances are broken down into management limits by business unit, product, portfolio or entity where useful (CPG 220 para 56). Management limits must sit inside Board tolerances.
- **Decisions.** Business cases, new products, material changes, acquisitions and material service provider arrangements must include an assessment against this Statement (CPG 220 para 51). A proposal that would take a risk outside appetite needs Board approval before it proceeds.
- **Delegations.** Delegations of authority for credit, underwriting, investment and expenditure are consistent with the tolerances.
- **Business planning.** The Statement is developed and reviewed as part of the strategic and business planning process (CPG 220 para 48), and the plan should be achievable within appetite.
- **Controls.** Each material risk has key controls mapped to it in the risk and control assessment, with testing frequency matched to materiality (CPS 230 para 29).
- **Remuneration.** Breaches of appetite and risk outcomes are considered in performance and variable remuneration outcomes under the RiskFA Remuneration Policy (CPS 511 where it applies).
- **Communication.** Staff are given a summary of the Statement relevant to their role (CPG 220 para 50).

16. Monitoring and reporting

Second line monitors the risk profile against this Statement and reports to management and the Board. Reports focus on what has changed, why, and what is being done.

Report	Audience	Frequency	Content
Risk appetite dashboard	[Executive Risk Committee]	[Monthly]	Status of every metric (Green / Amber / Red), trends, new triggers and breaches, actions and owners
Risk appetite report	[Board Risk Committee]	[Quarterly]	Overall risk profile against appetite by category; all Red metrics and Amber metrics for more than [2] periods; key control effectiveness; emerging risks; CRO view

Report	Audience	Frequency	Content
Breach notification	[Board Risk Committee chair]	As it happens (section 17)	Any Red breach or zero-tolerance matter
Annual appetite review	[Board]	[Annually]	Recommended changes to the Statement (section 18)

Reports must allow the Board to see the overall risk profile against appetite and capital strength, and to be satisfied that management is interpreting and applying appetite appropriately (CPG 220 para 49). The CRO gives an independent view in each Board Risk Committee report. Data used for appetite metrics must be accurate and timely; known data limitations are stated in the report (CPS 220 para 25).

17. Escalation when a trigger or tolerance is breached

CPS 220 para 28(d) requires a process for monitoring each tolerance and acting when it is breached. Where a risk is outside tolerance, APRA expects a plan to be developed and implemented promptly to bring it back within tolerance (CPG 220 para 59).

Status	Who is told, and when	What must happen
Amber (trigger reached)	Risk owner tells the [CRO] within [5 business days] ; reported at the next [Executive Risk Committee]	Risk owner records the cause and an action plan to return to Green, or explains why no action is needed. Second line challenges. If Amber persists for [2] reporting periods, it is reported to the [Board Risk Committee] .
Red (tolerance breached)	Risk owner tells the [CRO] and accountable executive within [24 hours] ; CRO tells the [Board Risk Committee chair] within [2 business days]	Record an issue (and an incident where loss or harm occurred) under the RiskFA Incident & Issues Management Standard, rated at least [High] . Agree a remediation plan within [10 business days] with a date to return within tolerance. The Board either approves the plan or decides to accept the risk temporarily, with a review date.

Status	Who is told, and when	What must happen
Zero-tolerance matter	Immediately (within [1 hour]) to the [CRO] , [General Counsel] and [CEO] ; Board Risk Committee chair within [24 hours]	Treat as an incident rated at least [High] , usually Critical; contain; preserve evidence; assess regulatory notifications; apply the RiskFA Consequence Management Framework.
Critical operation outside tolerance	Incident escalation as Critical; APRA within 24 hours (CPS 230 para 41)	Report the failure and a remediation plan to the Board (CPS 230 para 40).

Regulatory notification. Compliance assesses every Red breach to decide whether it is, or forms part of, a significant breach of or material deviation from the risk management framework, which must be notified to APRA within 10 business days (CPS 220 para 53; SPS 220 para 35). A tolerance breach is not automatically notifiable, but the decision and reasons must be recorded. Other notifications (for example reportable situations to ASIC) are assessed under the RiskFA Incident & Issues Management Standard.

Temporary excess. The Board may approve operating outside a tolerance for a defined period, for example during a planned transition, only with a written rationale, interim controls, an end date and reporting at each Board Risk Committee meeting. An approved excess remains reported as Red.

18. Review and approval

- The Statement is reviewed at least [annually], as part of the strategy and business planning cycle, and when there is a material change in strategy, risk profile, capital or liquidity position, regulation or the external environment (CPS 220 para 28(e); SPS 220 para 20(e)).
- The CRO leads the review with the first line, with input from the CFO on capital and liquidity, stress testing results and the [ICAAP / Financial Condition Report] where relevant.
- The [Board Risk Committee] reviews the draft and recommends it to the Board. The Board approves it (CPS 220 paras 9(a), 27; SPS 220 para 19).
- APRA-regulated institutions send APRA a copy on adoption and after any material revision, within 10 business days of Board approval (CPS 220 para 52).
- The annual review of the risk management framework and the comprehensive review at least every three years assess whether the framework, including this Statement, remains consistent with the Board's risk appetite (CPS 220 paras 44-47; SPS 220 paras 27-29).
- Changes to individual management limits within Board tolerances may be approved by the [CRO] and reported to the [Board Risk Committee].

19. Roles and responsibilities

Role	Responsibilities
Board	Sets risk appetite and approves this Statement; forms a view of whether risk culture supports operating within appetite (CPS 220 para 9(b)); approves tolerance levels for critical operations (CPS 230 para 21(b)); decides on Red breaches and temporary excesses; holds management to account.
Board Risk Committee	Reviews the Statement and recommends it to the Board; monitors the risk profile against appetite each [quarter]; oversees remediation of Red breaches; receives zero-tolerance escalations.
CEO and executive team	Run the business within appetite; consider appetite in strategy and decisions; ensure risk owners act on triggers and breaches.
Accountable persons (FAR, where applicable)	Take reasonable steps to keep their areas of responsibility within appetite, as part of their accountability obligations under the <i>Financial Accountability Regime Act 2023</i> .
Chief Risk Officer	Owns this Statement and leads its review; provides independent challenge on appetite, tolerances, metrics and risk owners' assessments; reports to the Board Risk Committee; escalates Red breaches; as head of the risk management function, notifies the Board of any significant breach of, or material deviation from, the risk management framework (CPS 220 para 37(g); SPS 220 para 24(f)).
Chief Financial Officer	Provides capital, liquidity and financial metrics, stress testing and the link to the business plan.
Head of Compliance / General Counsel	Assesses whether breaches are notifiable; owns compliance and regulatory metrics.
Risk owner	Owns the metrics for their risk; monitors them; acts on Amber and Red status; ensures key controls are effective.
Control owner	Operates and evidences the key controls that keep the risk within appetite; reports control failures.
Internal Audit	Provides independent assurance on whether the risk appetite framework is designed and operating effectively, including data quality and escalation.

Role	Responsibilities
All staff	Understand the parts of this Statement that apply to their role; speak up when they see risk outside appetite.

20. Three lines of accountability

Line	Who	Role in risk appetite
First line	Business units, operations, technology	Own and manage risk within appetite; operate key controls; measure and report metrics; act on triggers and breaches.
Second line	Risk and Compliance	Own this Statement and the metrics register; challenge calibration and status; monitor and report independently; escalate breaches.
Third line	Internal Audit	Independently assure the design and operation of the risk appetite framework.

21. Related documents

- the RiskFA Risk Management Framework and [\[Risk Management Strategy\]](#)
- The RiskFA Incident & Issues Management Standard
- [\[Business Plan\]](#), [\[ICAAP\]](#) and [\[Stress Testing Policy\]](#)
- the RiskFA Operational Risk Management Policy, the RiskFA Business Continuity Policy (including the register of critical operations and tolerance levels) and [\[Service Provider Management Policy\]](#)
- the RiskFA Cyber Security Policy, [\[Privacy Policy\]](#) and [\[AI Policy\]](#)
- the RiskFA Compliance and Breach Reporting Policy, the RiskFA Consequence Management Framework and the RiskFA Remuneration Policy
- APRA: CPS 220 / SPS 220 *Risk Management* and CPG 220; CPS 230 *Operational Risk Management* and CPG 230; CPS 234 *Information Security*; CPS 511 *Remuneration*; CPG 229 *Climate Change Financial Risks*
- Financial Stability Board: *Principles for an Effective Risk Appetite Framework* (18 November 2013)
- Standards: AS ISO 31000 *Risk management - Guidelines*; AS ISO/IEC 42001 *Information technology - Artificial intelligence - Management system*

Appendix A. Risk appetite metrics register template

Keep one row per metric. The register is the single source of the metrics, thresholds and owners referred to in this Statement.

Field	What to record	Example
Metric ID	Unique reference	[LIQ-01]
Risk category	From section 9	[Liquidity]
Appetite level	From the scale in section 6	[Minimal]
Metric	What is measured and how it is calculated	[Liquidity Coverage Ratio, APS 210 basis]
Level of approval	Board tolerance or management limit	[Board]
Direction	Higher is better, or lower is better	[Higher is better]
Green / Amber / Red	Target range, trigger level and tolerance	[$\geq 130\%$ / 115-130% / $< 115\%$]
Rationale	Why the levels were set (impact if breached, likelihood, capacity)	[Buffer above regulatory minimum covers [x] days of stressed outflows]
Key controls	The controls relied on to keep the metric in range	[Daily liquidity monitoring; contingency funding plan]
Data source and frequency	System or report, and how often measured	[Treasury system, daily]
Risk owner	One named accountable person	[Treasurer]
Current value and status	Latest result and Green / Amber / Red	[142%, Green]
Trend	Improving, stable or deteriorating	[Stable]
Breach history	Dates of Amber and Red status, linked issue IDs	[None]
Last reviewed / approved	Date and approver of current levels	[date, Board]

Appendix B. Glossary

Term	Meaning
Appetite scale	The five levels used in this Statement: Averse, Minimal, Cautious, Open, Receptive (section 6).
Green / Amber / Red	Status of a metric: within appetite / trigger level reached / tolerance breached (outside appetite).
Board tolerance	A risk tolerance approved by the Board in this Statement.
Management limit	A more detailed limit set by management inside a Board tolerance.
Key control	A control the organisation relies on most to keep a material risk within appetite.
Design effectiveness / operating effectiveness	Whether a control is designed to address the risk, and whether it works as intended over time.
Preventive, detective, corrective control	A control that stops an event, finds it quickly, or limits and fixes its impact.
Risk treatment	The process of selecting and implementing options to address risk, such as avoiding, reducing, sharing or accepting it (AS ISO 31000).
Risk capacity	The maximum risk the organisation can take before breaching regulatory, financial, operational or customer obligations.
Risk profile	The organisation's current level of risk at a point in time.
KRI	Key risk indicator: a metric tracked against trigger and tolerance levels.
Temporary excess	A Board-approved period of operating outside a tolerance, with interim controls and an end date (section 17).
Zero tolerance	A matter the organisation will never knowingly accept; every occurrence is escalated immediately (section 13).
CET1, PCA, ORFR, LCR, NSFR	Common Equity Tier 1 capital ratio (ADIs); Prescribed Capital Amount (insurers); Operational Risk Financial Requirement (RSE licensees); Liquidity Coverage Ratio and Net Stable Funding Ratio (ADIs). Defined in the relevant APRA prudential standards.

Term	Meaning
Critical operation, Incident, Issue, Breach, Material service provider	As defined in the RiskFA Incident & Issues Management Standard.

Appendix C. Annual review checklist

- Strategy and business plan for the coming period reviewed, and appetite confirmed as consistent with them.
- Every material risk has a statement, appetite level, at least one metric, a risk owner and key controls.
- Tolerances recalibrated using current risk capacity, capital and liquidity strength, stress testing and loss experience.
- Metrics that stayed Green with no movement for a year checked for relevance; metrics that were often Red checked for calibration and control effectiveness.
- Zero-tolerance matters confirmed.
- Critical operation tolerance levels confirmed with the RiskFA Business Continuity Policy.
- Changes in regulation, the external environment and emerging risks (for example AI, cyber, climate) considered.
- Internal Audit and comprehensive review findings addressed.
- Board Risk Committee recommendation and Board approval recorded.
- Copy sent to APRA within 10 business days of approval (APRA-regulated institutions).
- Summary communicated to staff.



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.](#)