

Operational Risk Management Policy

How an organisation identifies, assesses, controls, monitors and reports operational risk, keeps its critical operations within tolerance and manages its service providers, built on APRA CPS 230 (2026). 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 policy. This Policy sits under the RiskFA Risk Management Framework and uses its rating scale, risk taxonomy 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, set the thresholds and timeframes to match your size and risk appetite, delete obligations that do not apply to you, and approve the Policy through your governance process. Regulatory requirements are summarised as at October 2026, using the paragraph numbers of the 2026 reissue of APRA CPS 230: 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	Operational Risk Management Policy
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 regulation, the business, critical operations or material service providers, or a Critical incident
Parent document	RiskFA Risk Management Framework
Supporting documents	RiskFA Incident & Issues Management Standard; RiskFA Business Continuity Policy; RiskFA Crisis Management Plan; [Service Provider Management Policy] ; RiskFA Cyber Security Policy; RiskFA AI Risk Management Policy

1. Purpose

This Policy sets the minimum requirements for managing **operational risk** at [Organisation] : 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). It ensures that [Organisation] :

- identifies, assesses and manages its operational risks, with internal controls that are designed and operating effectively, and with monitoring and remediation;
- can continue to deliver its **critical operations** within **tolerance levels** through severe disruptions, with a credible business continuity plan (BCP); and
- manages the risks that come from using **service providers**, with a service provider management policy, formal agreements and robust monitoring.

These are the three key requirements of APRA Prudential Standard CPS 230 *Operational Risk Management* (CPS 230 objectives and para 11). For an AFS licensee that is not regulated by APRA, this Policy is part of the adequate risk management systems required by *Corporations Act 2001* s912A(1)(h) (section 21).

Operational risk management is not a separate framework. It is part of the risk management framework required by CPS 220 or SPS 220 (CPS 230 para 15) and is integrated into the overall framework and processes (para 17). This Policy therefore uses, and does not repeat, the governance, rating scale, controls method, RCSA and KRI rules in the RiskFA Risk Management Framework.

2. Scope and application

This Policy applies to all employees, contractors, directors and officers of [Organisation] and its subsidiaries; to all business units, products, services, processes, systems, data and locations; and to operational risks that arise at service providers and the parties they rely on. Operational risk is inherent in all products, activities, processes and systems (CPS 230 para 12).

If [Organisation] is	Main operational risk requirements (as at October 2026)
An ADI (including a foreign ADI's Australian branch) or authorised banking NOHC	CPS 230 in full (para 2(a)); CPG 230. Head of a group applies it on a group basis (paras 4–5). Operational risk capital under the ADI capital standards.
A general insurer, life company (including friendly societies and EFLICs), private health insurer, authorised or registered NOHC	CPS 230 in full (para 2(b)–(d)); CPG 230. Category C insurers and EFLICs apply it to their Australian branch operations only (para 3).
An RSE licensee (superannuation trustee)	CPS 230 in full, in respect of its business operations (para 2(e) and footnote 1); CPG 230; SPS 220; SPS 114 <i>Operational Risk Financial Requirement</i> .
An AFS licensee not regulated by APRA	<i>Corporations Act</i> s912A(1)(h) adequate risk management systems and s912A(1)(d) adequate resources; ASIC RG 104 (RG 104.33–RG 104.36 outsourcing; RG 104.59–RG 104.66 risk management systems).
A responsible entity of a registered scheme or corporate director of a CCIV	As for AFS licensees, plus ASIC RG 259 <i>Risk management systems of fund operators</i> , including operational risk (RG 259.113–RG 259.132).
Another financial services business	No prescribed operational risk standard. Adopt this Policy as good practice, scaled to the nature, size and complexity of the business.

CPS 230 sets baseline expectations for every APRA-regulated entity, and APRA expects significant financial institutions to have stronger practices commensurate with their size and complexity (CPG 230, *About this guide*). APRA may adjust or exclude a specific requirement for an entity (CPS 230 para 10). If [Organisation] is not APRA-regulated, read 'CPS 230 requires' in this Policy as 'industry best practice'.

3. Key definitions

Term	Meaning
Operational risk	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). It includes, but is not limited to, legal, regulatory, compliance, conduct, technology, data and change management risk (para 23).
Operational risk profile	The full set of [Organisation] 's operational risks, their inherent and residual ratings, the controls that manage them and their effectiveness, and their position against risk appetite, including open control gaps, weaknesses and failures (CPS 230 paras 15(b), 26, 30).
Operational resilience	The outcome of prudent operational risk management: the ability to manage and control operational risks, limit disruptions and maintain critical operations through disruptions (CPG 230 para 1).
Critical operation	A process undertaken by [Organisation] or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on its depositors, policyholders, beneficiaries or other customers, or its role in the financial system (CPS 230 para 34).
Tolerance levels	For each critical operation: the maximum period of time [Organisation] would tolerate a disruption; the maximum extent of data loss it would accept; and the minimum service levels it would maintain under alternative arrangements during a disruption (CPS 230 para 37).
Business continuity plan (BCP)	The plan or plans that set out how [Organisation] would maintain its critical operations within tolerance levels through disruptions, including disaster recovery planning for critical information assets. A BCP may include separate crisis management and disaster recovery plans (CPS 230 para 33(c) and footnote 12).
Service provider	Any party that provides a service to [Organisation] , including third parties, related parties and connected entities.
Material service provider	A service provider on which [Organisation] relies to undertake a critical operation, or that exposes it to material operational risk. A provider may be material because of one arrangement or several (CPS 230 para 48 and footnote 15).

Term	Meaning
Material arrangement	An arrangement on which [Organisation] relies to undertake a critical operation, or that exposes it to material operational risk (CPS 230 para 48).
Fourth party	A party that a service provider relies on in delivering services to [Organisation] (CPS 230 footnote 14).
Non-traditional service provider (NTSP)	APRA's term for a provider in a category listed in the Attachment to CPS 230 (for example government agencies, regulators, central banks, financial market exchanges, clearing and settlement facilities, payment systems and financial messaging infrastructures) (CPG 230 para 57).
Material offshoring arrangement	A material arrangement where the service is undertaken outside Australia, including where the provider is incorporated in Australia but performs the service offshore (CPS 230 footnote 16).
Key control, design effectiveness, operating effectiveness, RCSA, KRI, risk appetite, risk tolerance / limits	As defined in the RiskFA Risk Management Framework.
Incident, Near miss, Issue, Breach, Root cause, Extent of condition, Action, Customer remediation	As defined in the RiskFA Incident & Issues Management Standard.

4. Principles

1. **Start with critical operations.** Identify the critical operations, set their tolerance levels and map the processes and resources that deliver them; use this as the starting point for the operational risk profile (CPG 230 paras 2–3).
2. **Manage the full range.** Every operational risk, including legal, regulatory, compliance, conduct, technology, data and change management risk, has an owner and is managed end to end across the process (CPS 230 para 23).
3. **Controls must work.** Controls are designed, implemented and embedded in line with risk appetite, and tested for design and operating effectiveness at a frequency that matches the materiality of the risk (paras 28–29).
4. **Fix the cause.** Control gaps, weaknesses and failures stay in the risk profile until remediated, with clear accountability, assurance and root cause fixes (para 30).
5. **Plan for severe disruption.** Assume that severe but plausible events will happen, and be able to stay within tolerance levels when they do (paras 13, 42–43).
6. **Outsource the work, not the responsibility.** [Organisation] does not rely on a service provider unless it can still meet its obligations in full and manage the risks (para 14; RG 104.34).
7. **Proportionate.** The approach is appropriate to [Organisation] 's size, business mix and complexity (CPS 230 objectives).

5. Governance and the three lines of accountability

The Board is ultimately accountable for oversight of operational risk management, including business continuity and the management of service provider arrangements (CPS 230 para 19). [Organisation] applies the three lines of accountability set out in the RiskFA Risk Management Framework section 5.

Line	Who	Operational risk responsibilities
First line	Business units, operations, technology, procurement and the executives who lead them	Own and manage operational risk across the end-to-end process (CPS 230 para 23): identify and assess risks, design, operate and evidence controls, run first line control testing, monitor KRIs, record incidents and issues, own critical operations, BCPs and service provider arrangements.

Line	Who	Operational risk responsibilities
Second line	Operational Risk, Compliance, and specialist second line teams (for example information security, business continuity, third party risk)	Own this Policy and the methods; challenge risk and control assessments, critical operations, tolerance levels and materiality assessments; perform independent control testing; monitor the operational risk profile against appetite; assess APRA notifications; report independently to the executive and Board.
Third line	Internal Audit	Independently assure operational risk management; periodically review the BCP and give assurance to the Board (CPS 230 para 45); review any proposed material arrangement that outsources a critical operation and report regularly on compliance with the service provider management policy (para 61).

Delegations from, and reporting to, the Board and senior management are clear and documented, including for escalation of risks and issues, and the Board has reasonable assurance that there are no gaps in responsibilities (CPG 230 paras 7–8). The Board may delegate to senior management approval of more granular policies, tolerance levels and plans that sit beneath and align to Board-approved documents (CPG 230 para 13), and approval of non-material changes to the service provider management policy (CPG 230 para 11).

6. Roles and responsibilities

Role	Responsibilities
Board	Ultimately accountable for oversight of operational risk management (CPS 230 para 19). Ensures clear roles and responsibilities are set for senior managers (para 20). Oversees operational risk management and the effectiveness of key internal controls in keeping the operational risk profile within risk appetite, receives regular updates on the profile and ensures senior management acts on areas of concern (para 21(a)). Approves the BCP and tolerance levels, reviews testing results and oversees the execution of findings (para 21(b)). Approves the service provider management policy and reviews risk and performance reporting on material service providers (para 21(c)). Receives reports of any failure to meet tolerance levels, with a remediation plan (para 40).
Board Risk Committee	Recommends this Policy, the BCP, tolerance levels and the service provider management policy to the Board; reviews the operational risk profile, key control effectiveness, Critical and High incidents and issues, scenario analysis, BCP testing results and material service provider reporting [quarterly].
Board Audit Committee	Receives Internal Audit's assurance on the BCP and its regular reports on compliance of arrangements that outsource critical operations with the service provider management policy (CPS 230 paras 45, 61).
CEO and senior management	Responsible for operational risk management across the end-to-end process for all business operations (CPS 230 para 23). Provide clear and comprehensive information to the Board on the expected impacts on critical operations when the Board makes decisions that could affect their resilience (para 22). Act on areas of concern raised by the Board (para 21(a)). Receive control testing results (para 29) and reporting on material arrangements (para 59).
Accountable persons (FAR, where applicable)	Meet their FAR Act s21 obligations in their areas of responsibility. Approve, and review at least annually, the documented reasons where an operation on APRA's minimum list is not classified as critical, or a provider on APRA's minimum list is not classified as material (CPG 230 paras 18, 49).
Chief Risk Officer	Owns this Policy and the operational risk framework; leads the second line; provides effective challenge; reports independently on the operational risk profile to the Board Risk Committee; decides with Compliance on APRA notifications.

Role	Responsibilities
[Head of Operational Risk]	Maintains the methods, taxonomy mapping, RCSA, KRI and scenario analysis programs and the operational risk system; runs second line control testing; consolidates the operational risk profile.
Head of Compliance / General Counsel	Advises on legal, regulatory and compliance risk; maintains the obligations register; assesses breaches and makes or approves regulatory notifications under the RiskFA Incident & Issues Management Standard.
Chief Technology Officer	Maintains sound information and IT capability for current and projected business needs and critical operations, and monitors the age and health of information assets (CPS 230 para 24); owns disaster recovery for critical information assets.
Chief Information Security Officer (CISO)	Leads information security risk management under CPS 234 and the RiskFA Cyber Security Policy.
Critical operation owner	A named senior executive for each critical operation. Maintains its process and resource map, tolerance levels, BCP and test program; monitors performance against tolerance levels.
[Head of Business Continuity]	Maintains the BCP framework, the register of critical operations and the testing program under the RiskFA Business Continuity Policy.
Service provider (arrangement) owner	A named person accountable for each material arrangement: due diligence, the agreement, monitoring, risk management, BCP and exit planning (CPG 230 para 48(a)).
Risk owner and Control owner	As defined in the RiskFA Risk Management Framework section 6.
Incident, Issue and Action owners	As defined in the RiskFA Incident & Issues Management Standard.
All staff	Follow controls and procedures; report incidents, near misses, control weaknesses and service provider problems promptly.

7. Operational risk taxonomy

Operational risk is a Level 1 category in the RiskFA Risk Management Framework section 8.

[Organisation] uses the Level 2 risk types below for every operational risk, control, incident and issue. Each incident is also tagged with a loss event type, using the seven Basel II event types, so that loss data can be compared across the industry.

Level 2 risk type	Examples	Main Basel II event type
Process execution	Transaction errors, missed deadlines, manual workarounds, reconciliation failures, product or pricing errors	Execution, delivery and process management
People	Capacity, capability, key person dependency, supervision, workplace health and safety, employment practices	Employment practices and workplace safety
Technology	System outages, capacity, ageing or unsupported systems, failed changes, software defects	Business disruption and system failures
Information security and cyber	Cyber attack, unauthorised access, data loss, ransomware (RiskFA Cyber Security Policy)	External fraud; Business disruption and system failures
Data	Data quality, completeness, lineage, retention, misuse	Execution, delivery and process management
Change management	Poorly controlled change to products, processes, systems or organisation	Execution, delivery and process management
Third party and service provider	Provider failure or disruption, poor performance, fourth party failure, concentration, exit	Business disruption and system failures; Execution, delivery and process management
Fraud: internal	Staff fraud, collusion, unauthorised activity	Internal fraud
Fraud: external	Identity fraud, scams, payment fraud, cyber-enabled fraud	External fraud
Legal	Contract, litigation, enforceability of rights	Clients, products and business practices

Level 2 risk type	Examples	Main Basel II event type
Regulatory and compliance	Breach of law, licence condition or prudential standard; reporting failures	Clients, products and business practices
Conduct	Product design and distribution, sales practices, treatment of vulnerable customers, conflicts	Clients, products and business practices
Business continuity	Loss of site, people, systems or provider affecting critical operations	Damage to physical assets; Business disruption and system failures
Artificial intelligence and models	Model error, inappropriate use, bias, lack of explainability (RiskFA AI Risk Management Policy)	Execution, delivery and process management; Clients, products and business practices
Physical security and external events	Natural hazards, pandemic, terrorism, utility failure, physical damage	Damage to physical assets

The Risk Management Framework reports compliance and conduct risk as their own Level 1 categories for visibility. CPS 230 para 23 includes legal, regulatory, compliance and conduct risk in operational risk, so they are listed here too and are covered by this Policy's requirements for controls, testing, incidents and reporting. Use one classification in your system and map the other.

8. Operational risk appetite

CPS 230 para 15(b) requires an assessment of the operational risk profile with a defined risk appetite supported by indicators, limits and tolerance levels. The Board sets operational risk appetite in the RiskFA Risk Appetite Statement. As a minimum, it includes:

- a qualitative statement for each Level 2 risk type (for example [no appetite] for breaches of law, customer harm or disruption of a critical operation beyond tolerance);
- quantitative limits, for example net operational losses per year of no more than [\$X], and no more than [X] Critical incidents per year;
- the tolerance levels for each critical operation (section 17), which are Board-approved (para 21(b)); and
- KRIs with early warning triggers and limits for each Level 2 risk type and each critical operation (section 11).

Appetite breaches are escalated and recorded as issues under the RiskFA Risk Management Framework section 9.1.

9. The operational risk profile and risk assessment

[Organisation] maintains a comprehensive assessment of its operational risk profile (CPS 230 para 26). It is regularly updated to reflect changes in strategy, the risk environment and business mix, and is informed by scenario analysis (CPG 230 paras 21–22).

9.1 Required elements

Element	Requirement	Source
Information system	Maintain appropriate and effective information systems to monitor operational risk, compile and analyse operational risk data and facilitate reporting to the Board and senior management. [Organisation] uses [GRC system] as the single record of risks, controls, testing, KRIs, incidents, issues, critical operations and service providers.	CPS 230 para 26(a)
Critical operations mapping	Identify and document the processes and resources needed to deliver each critical operation (people, technology, information, facilities and service providers), the interdependencies across them, and the associated risks, obligations, key data and controls.	CPS 230 para 26(b); CPG 230 paras 19–20
Scenario analysis	Assess the potential impact of severe operational risk events, test operational resilience and identify the need for new or amended controls and other mitigation (section 12).	CPS 230 para 26(c)
Control weaknesses	Include identified control gaps, weaknesses and failures in the profile until they are remediated.	CPS 230 para 30
Incidents and near misses	Take incidents and near misses into account in assessing the profile and control effectiveness in a timely manner.	CPS 230 para 31

9.2 Risk and control self-assessment (RCSA)

Each business unit and each critical operation completes an RCSA using the RiskFA Risk Management Framework sections 10–13 and the steps in CPG 230 Table 2:

1. **Context:** consider the business environment and changes in the business.
2. **Critical operations:** identify the critical operations the unit supports and the processes

and resources needed to provide them.

3. **Risks:** identify and record operational risks, with causes, inherent and residual ratings on the common rating scale.
4. **Controls:** identify the controls, including those operated by related parties and service providers, and assess their effectiveness using test results, incidents, issues and KRIs.
5. **Risk appetite:** assess the residual position against appetite.
6. **Actions:** agree treatment or remediation for higher-rated risks and those outside appetite, or formally accept the risk under the Framework section 18.

RCSAs are refreshed at least **[annually]**, and when triggered by a Critical or High incident, a material change (section 13), a new or changed material arrangement, a KRI breach, or an audit or regulator finding. Second line challenges every RCSA before sign-off by the business unit executive.

10. Controls: design, implementation and testing

10.1 Design and implementation

[Organisation] designs, implements and embeds internal controls to mitigate its operational risks in line with its risk appetite and to meet its compliance obligations (CPS 230 para 28). To the extent possible, controls minimise the likelihood and impact of disruptions, particularly to critical operations (CPG 230 para 23). The control library should have a mix of preventive, detective and corrective controls and of automated and manual controls, and capture all controls, including those owned by related parties and service providers (CPG 230 para 24). Every Critical or High inherent risk has identified **key controls** (RiskFA Risk Management Framework section 12.2).

10.2 Monitoring and testing

Controls are regularly monitored, reviewed and tested for **design and operating effectiveness**, at a frequency commensurate with the materiality of the risks being controlled (CPS 230 para 29). Testing is conducted by staff independent of those with operational responsibility for the control (CPG 230 para 23).

Control	Minimum testing	Tested by
Key controls for Critical or High inherent risks, and key controls supporting a critical operation	Design and operating effectiveness at least [annually]	Second line or Internal Audit (independent of the control owner)

Control	Minimum testing	Tested by
Other key controls	At least every [2] years	First line quality assurance, with second line review of a sample
Other controls	At least every [3] years, or on a trigger	First line
Controls operated by material service providers	Through provider assurance reports, contractual audit rights or own testing, at least [annually]	Service provider owner, with second line review

- Testing uses consistent criteria across the organisation, and the rationale for each effectiveness rating is recorded (CPG 230 para 24(a), (h)).
- Control ratings (Effective, Partly effective, Ineffective) are as defined in the RiskFA Risk Management Framework section 12.3.
- Results of testing are reported to senior management, and gaps or deficiencies are rectified in a timely manner (CPS 230 para 29), by raising issues under the RiskFA Incident & Issues Management Standard.
- Control owners attest [quarterly] that their key controls operated, with evidence.
- A control is reassessed after an incident or near miss, a KRI breach, a process, system or provider change, or an audit or regulator finding.

11. Key risk indicators (KRIs)

KRIs support the risk appetite with indicators, limits and tolerance levels (CPS 230 para 15(b)) and give early warning of changes in risk or control effectiveness. They follow the RiskFA Risk Management Framework section 14: each KRI has an owner, a data source, a frequency, an early warning trigger (Amber) and a limit (Red) set in line with the Risk Appetite Statement. As a minimum there is at least [one] KRI for each Level 2 risk type in section 7, for each critical operation and for each material service provider. Appendix D lists common operational risk KRIs.

12. Scenario analysis

[Organisation] undertakes scenario analysis to identify and assess the potential impact of severe operational risk events, test its operational resilience and identify the need for new or amended controls and other mitigation strategies (CPS 230 para 26(c)).

- Scenarios are **severe but plausible**, cover the top [10] operational risks and every critical operation over a [three] -year cycle, and include, for example: a cyber attack disabling a critical operation; failure or prolonged outage of a material service provider or a key fourth party; loss of a main site; a large internal or external fraud; a major data corruption event; a failed major change; and a large customer remediation.
- Each scenario is run as a structured workshop with the risk owners, critical operation owners and specialists, using internal and external loss data, incidents and near misses. It records the assumptions, the estimated impact on each impact category, whether tolerance levels would be breached, and the controls that would and would not work.
- Results update the operational risk profile, risk ratings, controls, BCPs and the BCP testing program (section 17.4), and are reported to the Board Risk Committee.
- Scenario analysis is coordinated with enterprise stress testing (RiskFA Risk Management Framework section 15) and with recovery and exit planning where it applies: business continuity planning must be consistent with, and not conflict with or undermine, recovery and exit planning (CPS 230 para 17).

13. Change management, new products and strategic decisions

- [Organisation] assesses the impact of its business and strategic decisions on its operational risk profile and operational resilience as part of business and strategic planning, including the impact of new products, services, geographies and technologies (CPS 230 para 25).
- Before the Board makes a decision that could affect the resilience of critical operations, senior management gives it clear and comprehensive information on the expected impacts (para 22).
- Before providing a material service to another party (for example to a related entity or a client), [Organisation] conducts a comprehensive risk assessment to ensure it can continue to meet its prudential obligations after entering into the arrangement (para 27).
- New products, material changes to products, processes or systems, new or materially changed material arrangements, outsourcing, offshoring and acquisitions follow the [New Product and Change Approval Policy]: an operational risk assessment using this Policy, review of the effect on critical operations, tolerance levels, BCPs and material service providers, second line review, and approval at the right level before launch.
- Technology changes follow the [Change Management Standard]: risk-based approval, testing, segregation between development and production, a back-out plan, and post-implementation review. Failed changes are recorded as incidents.

14. Managing specific operational risks

14.1 People

- Capacity and capability are planned for each critical operation, with key person dependencies identified and covered by succession plans and cross-training.
- Pre-employment screening, segregation of duties, mandatory leave or rotation for high-risk roles, and conflicts of interest declarations are key controls for people and fraud risk.
- Workplace health and safety, employment practices and remuneration consequences are managed under the relevant policies; risk and control outcomes are considered in performance and remuneration (CPS 511 where it applies).

14.2 Process

- Processes supporting critical operations and material risks are documented, owned and reviewed at least every [2] years.
- Manual workarounds, end-user computing tools (for example spreadsheets) used in key processes, and reconciliations are inventoried and controlled.

14.3 Technology and information security

- [Organisation] maintains appropriate and sound information and IT capability to meet current and projected business requirements and to support critical operations and risk management (CPS 230 para 24).
- The age and health of information assets are monitored (para 24): technology owners report end-of-support assets, technical debt, capacity and resilience gaps for systems that support critical operations.
- Information security meets CPS 234 (para 24) and is managed under the RiskFA Cyber Security Policy and the RiskFA Cyber Incident Response Plan.
- Disaster recovery plans for critical information assets are part of the BCP (para 33(c)), and recovery time and recovery point objectives support the tolerance levels (section 17).

14.4 Data

- Data risk is managed as part of operational risk (CPS 230 para 23). The key data needed for each critical operation is identified (para 26(b)).
- [Organisation] applies a systematic approach to data quality, validation, life-cycle management and data quality assurance, using APRA CPG 235 *Managing Data Risk* as guidance.
- Personal information is handled under the [Privacy Policy] and the RiskFA Data Breach Response Plan.

14.5 Legal, regulatory and compliance

- Legal, regulatory and compliance risk are managed as operational risks (CPS 230 para 23), supported by an obligations register that maps each obligation to its owner and controls.
- Breaches are assessed and notified under the RiskFA Incident & Issues Management Standard. Contracts are reviewed by [Legal] before signing, using standard terms where possible.

14.6 Conduct

- [Organisation] sets and maintains appropriate standards for conduct and compliance (CPS 230 para 11(a)). Conduct risks are assessed in the RCSA and monitored through complaints, product reviews and quality assurance, under the [Conduct Risk Policy].

14.7 Fraud

- Internal and external fraud are assessed in the RCSA and through a [biennial] fraud risk assessment. Key controls include segregation of duties, approval limits, verification of payment and account changes, transaction monitoring, and access reviews.
- Suspected fraud is recorded and handled under the RiskFA Incident & Issues Management Standard and the [Fraud and Corruption Control Policy]. Suspicious matters are reported under the AML/CTF program.
- Fund operators should treat fraud risk as part of their risk management systems (RG 259.129–RG 259.132).

14.8 Artificial intelligence and models

- The use of AI and models is assessed and controlled under the RiskFA AI Risk Management Policy, using the existing controls for models, data, change, service providers and information security. AI used in or for a critical operation is included in the critical operation's process and resource map.

14.9 External events and physical security

- Sites, facilities and utilities supporting critical operations are assessed for natural hazards and other external events, and covered by the BCP and physical security controls.
- Insurance (for example property, business interruption, crime and professional indemnity) is reviewed [annually] as a risk transfer measure, but does not replace controls.

15. Operational risk incidents

Operational risk incidents and near misses are identified, escalated, recorded and addressed in a timely manner, and are taken into account in the operational risk profile and the assessment of control effectiveness (CPS 230 para 31). All of this is done under the **RiskFA Incident & Issues Management Standard**, which sets the lifecycle (detect, escalate, contain, respond, review, as in CPG 230 Table 3), rating, timeframes, root cause analysis and closure rules.

- Every incident is linked to the affected risks, controls, critical operations and service providers, so that the risk profile accurately reflects control weaknesses (CPG 230 para 29).
- Gross loss, recoveries and net loss are recorded for every incident with a financial impact, with the loss event type (section 7), to build an internal loss database.
- Incidents at service providers that affect [Organisation] are recorded as [Organisation]'s own incidents.
- **APRA notification (CPS 230 para 32):** APRA must be notified as soon as possible and not later than **72 hours** after becoming aware of an operational risk incident that [Organisation] determines is likely to have a material financial impact or a material impact on its ability to maintain its critical operations. The materiality decision is made and recorded within [24 hours] of identification, as set out in the RiskFA Incident & Issues Management Standard section 10. An information security incident notified under CPS 234 need not be notified again under CPS 230 (footnote 11).

16. Remediating control weaknesses

[Organisation] remediates material weaknesses in its operational risk management, including control gaps, weaknesses and failures, with clear accountability and assurance, addressing root causes in a timely manner (CPS 230 para 30).

- Each weakness is raised as an issue with one owner, a rating and an action plan under the RiskFA Incident & Issues Management Standard section 11.

- Responses often combine tactical measures (temporary controls or monitoring) with strategic fixes (changes to processes, people or systems) (CPG 230 para 28).
- Extended delays and unwarranted extensions to target closure dates are avoided (CPG 230 para 29); extensions follow the Standard's approval rules.
- Issues stay in the operational risk profile, and the affected controls are rated Partly effective or Ineffective, until the issue is closed as complete and effective.
- Where [Organisation] has identified material weaknesses, it keeps APRA informed of remediation progress (CPG 230 para 5). APRA may require an independent review, a remediation program, additional capital or licence conditions (CPS 230 para 18); for ADIs and insurers, APRA generally expects additional operational risk capital until remediation is complete (CPG 230 para 6), and for RSE licensees APRA may require an operational risk financial requirement target amount (CPS 230 footnote 7).

17. Business continuity

This section sets the minimum CPS 230 requirements. The **RiskFA Business Continuity Policy** sets out how they are met (business impact analysis, plans, crisis management, testing and recovery). [Organisation] must (CPS 230 para 33):

1. define, identify and maintain a register of its critical operations;
2. take reasonable steps to minimise the likelihood and impact of disruptions to critical operations;
3. maintain a credible BCP that sets out how it would maintain critical operations within tolerance levels through disruptions, including disaster recovery planning for critical information assets;
4. activate the BCP if needed in a disruption; and
5. return to normal operations promptly after a disruption is over.

17.1 Identifying critical operations

- Critical operations focus on outward-facing services to depositors, policyholders, beneficiaries and other customers, and the entity's role in the financial system (CPG 230 para 15). Consider operations whose disruption would have a direct or indirect material adverse impact on customers, or could affect the broader financial system (CPG 230 para 16).
- As a minimum, unless [Organisation] can justify otherwise, the following are critical operations (CPS 230 para 35): **ADIs**: payments, deposit-taking and management, custody, settlements and clearing; **insurers**: claims processing; **RSE licensees**: investment management and fund administration; **all entities**: customer enquiries and the systems and infrastructure needed to support critical operations.
- Critical functions determined under CPS 900 *Resolution Planning* are also classified as critical operations (CPG 230 para 17). APRA may require an operation to be classified as critical (CPS 230 para 36).
- Where an operation on the minimum list is not classified as critical, the reasons are documented, approved by an accountable person and reviewed at least annually (CPG 230 para 18).
- The register of critical operations holds at least the fields in Appendix B.

17.2 Tolerance levels

For each critical operation [Organisation] sets tolerance levels for (CPS 230 para 37): (a) the **maximum period of time** it would tolerate a disruption; (b) the **maximum extent of data loss** it would accept; and (c) the **minimum service levels** it would maintain under alternative arrangements. CPG 230 Table 4 links these to the maximum allowable disruption and recovery time objective, the recovery point objective and the recovery level objective.

- In setting tolerance levels, consider the impact on customers and stakeholders, the financial and reputational impact on [Organisation] and on the broader financial system, legal and regulatory requirements (including any tolerance set by APRA), and recovery objectives (CPG 230 para 32).
- Tolerance levels are approved by the Board (CPS 230 para 21(b)), and reassessed as lessons are learned from actual disruptions, testing and scenario analysis (CPG 230 para 33). APRA may require changes or set tolerance levels (CPS 230 para 38).
- Compliance with tolerance levels is monitored, and any failure to meet them is reported to the Board with a remediation plan (CPS 230 para 40).

17.3 The business continuity plan

The BCP must include (CPS 230 para 39): the register of critical operations and tolerance levels; triggers to identify a disruption and prompt activation, and arrangements to direct resources; actions to maintain critical operations within tolerance levels; an assessment of execution risks, required resources and preparatory measures, including key internal and external dependencies; and a communications strategy. [Organisation] maintains the capabilities to execute the BCP, including access to people, resources and technology; capabilities provided by another party must meet the service provider requirements in section 18 (para 40 and footnote 13). The BCP is linked to the disaster recovery, liquidity management, information security incident and crisis management plans (CPG 230 para 36).

17.4 Testing, review and assurance

- A systematic testing program covers all critical operations and includes an **annual business continuity exercise**, testing the BCP's effectiveness and the ability to meet tolerance levels in a range of severe but plausible scenarios (CPS 230 para 42). All critical operations would typically be considered over a multi-year cycle, for example three years (CPG 230 para 37).
- The program is tailored to [Organisation]'s material risks and includes disruptions to services provided by material service providers and scenarios where contingency arrangements are required (CPS 230 para 43). APRA may require an APRA-determined scenario.
- Test reports state the scope (including critical operations and tolerance levels tested), what was demonstrated (including whether tolerance levels were met), and issues, root causes and remediation (CPG 230 para 38). The Board reviews testing results and oversees the execution of findings (CPS 230 para 21(b)).
- The BCP is updated as necessary on an annual basis for changes in legal or organisational structure, business mix, strategy or risk profile, or for shortcomings found in review and testing (para 44).
- Internal Audit periodically reviews the BCP and gives the Board assurance that it is a credible plan and that testing is adequate and has been conducted satisfactorily (para 45).

17.5 Disruption outside tolerance

If a critical operation is disrupted **outside tolerance**, [Organisation] must notify APRA as soon as possible and not later than **24 hours** after, covering the nature of the disruption, the action taken, the likely impact on business operations and the timeframe for returning to normal operations (CPS 230 para 41). The failure is also reported to the Board with a remediation plan (para 40) and recorded as a Critical incident.

18. Management of service provider arrangements

[Organisation] does not rely on a service provider unless it can ensure that it can continue to meet its prudential obligations in full and effectively manage the associated risks (CPS 230 para 14). Where it uses a service provider, it still owns and is responsible for managing the risk (CPG 230 para 44). The detailed requirements are in the [Service Provider Management Policy], which the Board approves (para 21(c)).

18.1 The service provider management policy

CPS 230 paras 46–47 require a comprehensive service provider management policy covering how [Organisation] identifies material service providers and manages service provider arrangements, including: the approach to entering into, monitoring, substituting and exiting agreements with material service providers; managing the risks associated with material service providers; and managing the risks of fourth parties that material service providers rely on to deliver a critical operation. CPG 230 para 45 adds that it would usually cover accountable persons' roles, selection and due diligence, materiality methodology, on-boarding and exit, BCP and alternative arrangements, issues and escalation, vetting of key personnel, and oversight of providers and service levels.

18.2 Material service providers and the register

- [Organisation] identifies and maintains a **register of material service providers** and manages the material risks of using them (CPS 230 para 48). The register holds at least the fields in Appendix C, and is submitted to APRA **annually** (para 50).
- As a minimum, unless [Organisation] can justify otherwise, providers of these services are material (para 49): **ADIs**: credit assessment, funding and liquidity management, mortgage brokerage; **insurers**: underwriting, claims management, insurance brokerage, reinsurance; **RSE licensees**: fund administration, custodial services, investment management, arrangements with promoters and financial planners; **all entities**: risk management, core technology services, internal audit.
- Arm's length transactions or intermediation are not automatically material unless they meet the para 48 criteria (CPG 230 para 47). Where a provider on the minimum list is not classified as material, the reasons are documented, approved by an accountable person and reviewed at least annually (CPG 230 para 49).
- Cohorts of providers whose aggregate impact is material, but where no single provider is, have additional processes and controls (CPG 230 para 51). APRA may require a provider or arrangement to be classified as material (CPS 230 para 51).

18.3 Before entering into or materially changing a material arrangement

- Undertake appropriate due diligence, including an appropriate selection process and an assessment of the provider's ability to provide the service on an ongoing basis (CPS 230 para 52(a)).
- Assess the financial and non-financial risks of reliance on the provider, including geographic location and concentration of the provider or the parties it relies on (para 52(b)), against risk appetite: services that must stay in-house, country, supplier, concentration and reputational risk (CPG 230 para 54), and for offshore providers, continuity, information security, control, compliance and APRA access (CPG 230 para 55).
- Have Internal Audit review any proposed material arrangement that outsources a critical operation, before the final decision (CPS 230 para 61; CPG 230 para 56).

18.4 Formal agreements

Every material arrangement has a formal legally binding agreement that, at a minimum (CPS 230 para 53): specifies the services and service levels; sets out the rights, responsibilities and expectations of each party, including ownership of assets, ownership and control of data, dispute resolution, audit access, liability and indemnity; ensures [Organisation] can meet its legal and compliance obligations; requires the provider to notify its use of other material service providers it materially relies on (sub-contracting); makes the provider liable for failures of its sub-contractors; includes a force majeure provision stating which parts continue; and includes termination rights for all or part of the arrangement (for RSE licensees, including where continuing would be inconsistent with the duty to act in beneficiaries' best financial interests). The agreement also allows APRA access to documentation, data and information, gives APRA the right to an on-site visit, and requires the provider not to impede APRA (para 54).

18.5 Managing each material arrangement

- Identify and manage risks to the provider's ability to provide the service on an ongoing basis, and risks to [Organisation] from the arrangement, such as step-in or contagion risk (CPS 230 para 55(a)–(b)).
- Ensure [Organisation] can execute its BCP if needed, and conduct an orderly exit (para 55(c)–(d)). Each material arrangement has a documented [exit plan], tested or reviewed at least [every 2 years].
- Monitor and report to senior management, commensurate with the nature and usage of the service, including regular assessment of performance against service levels, effectiveness of controls over the provider's risks, and compliance of both parties with the agreement (para 59). Periodic reviews also cover incidents, information security and business continuity capability, and strategic changes (CPG 230 para 53).
- Take reasonable steps to list the fourth parties involved in delivering each critical operation (CPG 230 para 48(c)), and satisfy itself that material providers' risk management and BCPs, including BCP testing, are robust (CPG 230 paras 39, 50).
- Report risk and performance on material service providers to the Board (para 21(c)).

18.6 Exempt categories (non-traditional service providers)

For a material arrangement with a provider in a category listed in the Attachment to CPS 230 (government agencies, regulators, central banks, financial market exchanges, operators of clearing and settlement facilities, operators of payment systems and schemes, and financial messaging infrastructures) that uses standardised terms or is not documented in a formal agreement, [Organisation] need not comply with paras 53, 54, 55(d), 59(a) and 59(c) (CPS 230 para 57). APRA may grant other exemptions by written notice (para 58). Exemptions should be applied only to the paragraphs that cannot reasonably be met, and [Organisation] still assesses materiality, performs due diligence where there is a choice, monitors the risks using public information and its own incident data, includes the arrangement in critical operations mapping and BCPs, and lists it on the register (CPG 230 paras 60–61 and Table 5).

18.7 Notifications about service providers

- Notify APRA as soon as possible and not more than **20 business days** after entering into or materially changing an agreement for a service on which [Organisation] relies to undertake a critical operation (CPS 230 para 60(a)).
- Notify APRA **before** entering into any material offshoring arrangement, or when a significant change is proposed, including where data or personnel relevant to the service will be located offshore (para 60(b)).

19. Notifications to APRA

Notifications are made electronically using the form on APRA's website (CPG 230 para 14). Where a matter falls into two categories, the shorter timeframe applies (CPG 230 Table 1, note). Decisions to notify or not are recorded with reasons under the RiskFA Incident & Issues Management Standard.

Obligation (CPS 230, 2026)	Trigger	Timeframe
Operational risk incident (para 32)	An incident [Organisation] determines is likely to have a material financial impact, or a material impact on its ability to maintain critical operations. Not needed if already notified under CPS 234 (footnote 11).	As soon as possible, and not later than 72 hours after becoming aware
Disruption outside tolerance (para 41)	A critical operation has been disrupted outside tolerance. Cover the nature of the disruption, action taken, likely impact and time to return to normal.	As soon as possible, and not later than 24 hours after

Obligation (CPS 230, 2026)	Trigger	Timeframe
Material service provider register (para 50)	Annual submission of the register, using APRA's template (its preferred format) through APRA Connect as APRA directs.	Annually , by the date APRA sets
Critical operation service agreement (para 60(a))	Entering into or materially changing an agreement for a service relied on to undertake a critical operation.	As soon as possible, and not more than 20 business days after
Material offshoring (para 60(b))	Entering into a material offshoring arrangement, or a significant proposed change, including data or personnel moving offshore.	Before entering into it, or when the change is proposed

Other notifications that may arise from the same event (for example CPS 234 para 35 information security incidents, breach reporting to ASIC, notifiable data breaches) are in the RiskFA Incident & Issues Management Standard section 10.

20. Reporting

Report	Audience	Frequency	Content
Operational risk profile report	Board Risk Committee and Board	[Quarterly]	Operational risk profile against appetite (para 21(a)); key control effectiveness and testing results; Critical and High incidents, losses and near misses; open issues and overdue actions; KRIs at Amber or Red; APRA notifications; scenario analysis results; CRO's view
Critical operations and resilience report	Board Risk Committee and Board	[Quarterly] , and after any disruption	Performance against tolerance levels; any failure to meet them with a remediation plan (para 40); BCP testing results and execution of findings (para 21(b)); technology health of systems supporting critical operations
Material service provider report	Board Risk Committee and Board	[Half-yearly]	Risk and performance of material service providers (para 21(c)); changes to the register; concentration and fourth party risks; notifications made
Internal Audit reports	Board Audit Committee	Per audit plan	Assurance on the BCP (para 45); compliance of arrangements that outsource critical operations with the service provider management policy (para 61)
Management report	Executive Risk Committee and senior management	[Monthly]	As above, in more detail, plus control testing results (para 29) and reporting on material arrangements (para 59)

Board information is targeted and timely (CPG 230 para 12). Bad news is reported promptly and never held until the next scheduled report.

21. AFS licensees and fund operators not regulated by APRA

If **[Organisation]** is an AFS licensee that is not a body regulated by APRA, it must have adequate risk management systems (*Corporations Act* s912A(1)(h)) and adequate financial, technological and human resources (s912A(1)(d)). ASIC's guidance maps to this Policy as follows:

ASIC expectation	Reference	Where met in this Policy
Risk management systems based on a structured and systematic process; identify and evaluate risks, focusing on risks that adversely affect consumers or market integrity; establish controls; fully implement and monitor them to ensure they are effective	RG 104.62	Sections 7–12
Systems that depend on the nature, scale and complexity of the business and adapt as it changes	RG 104.63–RG 104.64	Sections 2, 9, 13
Outsourcing: the licensee remains responsible; due skill and care in choosing providers; monitoring ongoing performance; dealing with breaches of service levels or obligations; different risk management measures for outsourced functions	RG 104.34, RG 104.36, RG 104.65	Section 18
Business continuity plan; annual review of risk management measures	RG 104 Table 3	Sections 17, 22
Fund operators: operational risk (legal and compliance, technology, people and key persons, outsourcing, transitioning the business, cyber, employee conduct, fraud)	RG 259.113–RG 259.132	Sections 7, 14, 17, 18
Fund operators: skills to oversee external service providers; risk indicators; review of risk management systems at least annually	RG 259.23, RG 259.77, RG 259.89	Sections 11, 18, 22

For these organisations, the APRA notification requirements in sections 15, 17.5, 18.7 and 19 do not apply; ASIC reportable situations and other obligations in the RiskFA Incident & Issues Management Standard still do. Market participants also have ASIC market integrity rule obligations for technological and operational resilience (Chapter 8B of the ASIC Market Integrity Rules (Securities Markets) 2017 and (Futures Markets) 2017).

22. Review and assurance

- Operational risk management, covering every element of CPS 230 para 15, is included in the annual and comprehensive reviews of the risk management framework under CPS 220 (paras 44–45) or SPS 220 (paras 27–28) (CPS 230 para 16). AFS licensees review their risk management systems at least annually (RG 104 Table 3; RG 259.89).
- Internal Audit's plan covers operational risk management, including control testing, the BCP (CPS 230 para 45), proposed outsourcing of critical operations and compliance with the service provider management policy (para 61), on a risk-based cycle of no more than [3] years.
- The CRO reports [annually] to the Board Risk Committee on the effectiveness of this Policy, coverage of RCSAs, control testing, scenario analysis and BCP testing, and the CPS 230 requirement map (Appendix A).

23. Accountability and compliance with this Policy

- Every operational risk, key control, critical operation and material arrangement has a named owner. For FAR accountable entities, these responsibilities are consistent with accountability statements and the accountability map.
- Breaches of this Policy (for example a material arrangement entered into without due diligence or a formal agreement, untested key controls, or a missed APRA notification) are recorded as issues and managed under the RiskFA Consequence Management Framework.
- Exemptions need the written approval of the CRO, are time-limited and are reported to the Board Risk Committee. An exemption cannot override a legal or prudential requirement.

24. Related documents

- RiskFA Risk Management Framework and RiskFA Risk Appetite Statement
- RiskFA Incident & Issues Management Standard
- RiskFA Business Continuity Policy and RiskFA Crisis Management Plan
- RiskFA Cyber Security Policy, RiskFA Cyber Incident Response Plan and RiskFA Data Breach Response Plan
- RiskFA AI Risk Management Policy
- [Service Provider Management Policy] , [New Product and Change Approval Policy] , [Change Management Standard] , [Fraud and Corruption Control Policy] , [Conduct Risk Policy] , [Privacy Policy]
- APRA: CPS 230 *Operational Risk Management* (determination No. 1 of 2026) and CPG 230 (July 2026); CPS 220 and SPS 220 *Risk Management*; CPS 234 *Information Security*; CPS 190 *Recovery and Exit Planning*; CPS 900 *Resolution Planning*; SPS 114 *Operational Risk Financial Requirement*; CPS 511 *Remuneration*; CPG 235 *Managing Data Risk*; APRA Material Service Provider Register Template (2026)
- Legislation: *Corporations Act 2001* s912A; *Financial Accountability Regime Act 2023*
- ASIC: RG 104 *AFS licensing: Meeting the general obligations*; RG 259 *Risk management systems of fund operators*
- Standards: AS ISO 31000 *Risk management*, ISO 22301 *Business continuity management systems*

Appendix A. CPS 230 requirement map

Paragraph numbers are those of CPS 230 as reissued in 2026 (determination No. 1 of 2026, in force 1 July 2026). Use the right-hand column to show where each requirement is met.

Requirement	CPS 230 para	Where met
Key principles: manage operational risk, conduct and compliance standards; critical operations within tolerance; service provider risk	11	Sections 1, 4
Identify, assess and manage operational risk	12	Sections 7–9
Prevent disruption, adapt, return to normal	13	Section 17

Requirement	CPS 230 para	Where met
Do not rely on a provider unless obligations can be met	14	Section 18
Operational risk elements of the risk management framework	15(a)–(f)	Sections 5–18
Review of operational risk management	16	Section 22
Integration; BCP consistent with recovery and exit planning	17	Sections 1, 12
APRA powers where material weaknesses exist	18	Section 16
Board accountability	19	Sections 5–6
Roles and responsibilities for senior managers	20	Section 6
Board oversight: risk profile and key controls; BCP and tolerances; service provider policy and reporting	21(a)–(c)	Sections 6, 17, 18, 20
Senior management information on critical operations impacts	22	Sections 6, 13
Full range of operational risks; end-to-end responsibility	23	Sections 7, 14
IT capability; age and health of information assets; CPS 234	24	Section 14.3
Impact of business and strategic decisions, new products, services, geographies, technologies	25	Section 13
Comprehensive assessment of the risk profile: information systems; critical operations mapping; scenario analysis	26(a)–(c)	Sections 9, 12
Risk assessment before providing a material service to another party	27	Section 13
Design, implement and embed controls	28	Section 10.1

Requirement	CPS 230 para	Where met
Monitor, review and test controls; report results; rectify gaps	29	Section 10.2
Remediate material weaknesses; keep in profile until remediated	30	Section 16
Identify, escalate, record and address incidents and near misses	31	Section 15
Notify APRA of material operational risk incidents (72 hours)	32	Sections 15, 19
Business continuity obligations	33	Section 17
Critical operations definition and minimum list	34–36	Section 17.1; Appendix B
Tolerance levels	37–38	Section 17.2
BCP contents	39	Section 17.3
BCP capabilities; monitor tolerance levels; report failures to the Board	40	Sections 17.2, 17.3
Notify APRA of disruption outside tolerance (24 hours)	41	Sections 17.5, 19
BCP testing program, annual exercise, severe but plausible scenarios	42–43	Section 17.4
Annual BCP update	44	Section 17.4
Internal Audit review of the BCP	45	Sections 5, 17.4, 22
Service provider management policy and contents	46–47	Section 18.1
Material service providers, register, minimum list	48–49, 51	Section 18.2; Appendix C
Submit the register to APRA annually	50	Sections 18.2, 19
Due diligence and risk assessment before a material arrangement	52	Section 18.3

Requirement	CPS 230 para	Where met
Formal agreement contents, including APRA access	53–54	Section 18.4
Ongoing risk management, BCP and orderly exit for each material arrangement	55–56	Section 18.5
Exemptions for listed provider categories	57–58, Attachment	Section 18.6
Monitoring and senior management reporting on material arrangements	59	Section 18.5
Notify APRA of critical operation agreements (20 business days) and material offshoring (before)	60(a)–(b)	Sections 18.7, 19
Internal Audit review of outsourcing of critical operations; reporting on compliance	61	Sections 18.3, 20, 22

Appendix B. Critical operations register: minimum fields

Fields marked † are in CPG 230 para 31 or in APRA's 2026 Material Service Provider Register Template ('COs and Tolerances' and 'CO Exceptions' tabs). The others are good practice.

Field	Description
Critical operation name and ID †	From APRA's minimum list (CPS 230 para 35) or identified by [Organisation] ; sub-type where relevant
Description †	The outward-facing service, who receives it and why it is critical
Basis for classification	Minimum list, CPS 900 critical function, APRA requirement, or [Organisation] 's own assessment of material adverse impact
Accountable executive / accountable person	Critical operation owner
Maximum period of disruption tolerated †	In hours (APRA's template asks for a number in hours)
Maximum data loss accepted †	For example in time since the last recoverable point

Field	Description
Minimum service level under alternative arrangements †	For example [X%] of normal volume, or named priority services
Tolerance approval	Date approved by the Board, and date of last review
Processes, people, technology, information, facilities	From the process and resource map (CPS 230 para 26(b))
Material service providers and arrangements supporting it †	Linked to the material service provider register
Known fourth parties	Parties the providers rely on to deliver this operation
Key risks, obligations, key data and controls	Linked to the RCSA and control library
BCP and disaster recovery plan references	Including recovery time and recovery point objectives that support the tolerance levels
Testing	Last test date, scenario, whether tolerance levels were met, open findings
Disruptions	Incidents affecting the operation, and any disruption outside tolerance
Exclusions from the minimum list †	For any minimum-list operation not classified as critical: the reasons, approval by an accountable person and sign-off date (CPG 230 para 18)

Appendix C. Material service provider register: minimum fields

Fields marked † are in CPG 230 para 48 or in APRA's 2026 Material Service Provider Register Template ('MSP Details', 'MSP Register', 'MSP Exceptions' and 'Fourth Parties' tabs). APRA prefers its template but accepts another format. The others are good practice.

Field	Description
Provider legal entity name †	Business entity name
ABN † and Legal Entity Identifier (if available) †	Identifiers for the provider

Field	Description
Accountable person in [Organisation] †	Name and title of the person accountable for the provider and arrangement
Materiality driver †	Relied on to undertake a critical operation, and/or exposes [Organisation] to material operational risk (including by aggregation of several contracts)
Critical operation(s) supported †	One record for each critical operation the arrangement supports
Linked material risk †	The material risk in the risk profile the arrangement connects to (CPG 230 para 48(b))
Service covered †	Name of the service
Contract title †, or non-traditional service provider category †	The formal agreement, or the Attachment category where the para 57 exemption is used
Provider category †	From the minimum list in CPS 230 para 49, or other
Start date † and end date †	End date blank if there is none
Fourth parties †	Known fourth parties, the provider they support, the arrangement and the critical operation (optional in APRA's template; CPG 230 para 48(c))
Exclusions from the minimum list †	For any minimum-list category not on the register: the reasons and the risk sign-off date (CPG 230 para 49)
Location of service and data	Countries where the service is performed and data is held; whether it is a material offshoring arrangement
Related party or connected entity	Whether the provider is part of [Organisation] 's group
Due diligence and risk assessment	Date and result of the last assessment, inherent and residual rating
Agreement compliance	Whether the agreement meets CPS 230 paras 53–54, and any exemption relied on
Monitoring	Service level performance, control assurance received, last review date, open incidents and issues

Field	Description
BCP and exit	Provider BCP testing evidence, [Organisation] 's contingency arrangements and exit plan, date last reviewed
APRA notifications	Para 60(a) or 60(b) notifications made and dates

Appendix D. Operational risk KRIs

Examples of common KRIs. Choose those that fit [Organisation] 's risks, set the Amber and Red thresholds in line with the Risk Appetite Statement, and record an owner and data source for each. These are industry practice, not regulatory requirements.

Area	KRI	Example thresholds (Amber / Red)
Losses and incidents	Net operational losses, rolling 12 months	[\$X] / [\$Y]
Losses and incidents	Number of Critical or High incidents in the quarter	[1] / [2]
Losses and incidents	Incidents recorded later than required after identification	[5%] / [10%]
Controls	Key controls rated Partly effective or Ineffective	[5%] / [10%]
Controls	Key controls overdue for testing	[5%] / [10%]
Issues	High or Critical issue actions overdue	[1] / [3], or any more than [90 days] overdue
Critical operations	Disruptions to a critical operation (within tolerance) in the quarter	[1] / [3]; any disruption outside tolerance is Red
Critical operations	Critical operations not tested within the planned cycle	[1] / [2]
Technology	Systems supporting critical operations at or past end of support	[1] / [3]
Technology	Failed or emergency changes as a share of all changes	[3%] / [5%]

Area	KRI	Example thresholds (Amber / Red)
Information security	Critical vulnerabilities not patched within the target time	[X] / [Y] (RiskFA Cyber Security Policy)
Service providers	Material service providers missing agreed service levels	[1] / [2] in a quarter
Service providers	Material arrangements without a current due diligence review or exit plan	[1] / [3]
People	Voluntary staff turnover in teams supporting critical operations	[15%] / [20%] annualised
People	Key person roles without a trained successor	[2] / [5]
Fraud	Confirmed internal or external fraud losses, rolling 12 months	[\$X] / [\$Y]
Data	Data quality exceptions in key data for critical operations or regulatory reporting	[X] / [Y]
Compliance	Regulatory notifications lodged late	Any is Red
Change	Major changes implemented without completed operational risk assessment	Any is Red