

Business Continuity Policy

How to identify critical operations, set tolerance levels, plan for and test against severe disruption, and keep critical operations running within tolerance, aligned to APRA CPS 230 and ISO 22301. 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. 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 tolerance levels, timeframes and testing cycle to match your size, business mix and risk appetite, delete obligations that do not apply to you, and approve the Policy through your governance process. Keep printed or offline copies of the business continuity plans that sit under this Policy: in a severe disruption your systems and offices may not be available. 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	Business Continuity Policy
Organisation	[Organisation name]
Document owner	[Chief Risk Officer] (policy); [Chief Operating Officer] (business continuity program)
Approved by	[Board] , on the recommendation of the [Board Risk Committee] . The Board also approves the business continuity plan (BCP) and the tolerance levels for critical operations (CPS 230 para 21(b))
Version / date approved	[1.0] / [date]
Review cycle	At least [annually] , and after any material change in structure, business mix, strategy, risk profile or regulation, a disruption to a critical operation, or a significant test finding
Parent documents	The RiskFA Risk Management Framework; the RiskFA Operational Risk Management Policy
Plans under this Policy	[Business Continuity Plan(s)] , [Disaster Recovery Plans] , the RiskFA Crisis Management Plan, [Pandemic Plan] , the RiskFA Cyber Incident Response Plan (linked)

1. Purpose

This Policy sets the minimum requirements for how [Organisation] prepares for, responds to and recovers from disruptions, so that it can keep delivering its **critical operations within tolerance levels** through severe but plausible events. It ensures that:

- critical operations, and the people, technology, information, facilities and service providers they depend on, are identified and documented;
- the Board sets clear, measurable tolerance levels for disruption to each critical operation;
- credible business continuity plans exist, are kept up to date and can be activated quickly;
- plans are tested against severe but plausible scenarios, including the failure of material service providers, and weaknesses are fixed;

- the Board and APRA are told when a critical operation is disrupted outside tolerance; and
- customers, beneficiaries and the wider financial system are protected from the harm a prolonged disruption would cause.

The Policy supports [Organisation]'s obligations, where they apply, under APRA Prudential Standard CPS 230 *Operational Risk Management* (2026), which requires an APRA-regulated entity to maintain its critical operations within tolerance levels through severe disruptions (para 11(b)) and to have business continuity plans that are regularly tested with severe but plausible scenarios (para 15(e)). It follows APRA's guidance in CPG 230 *Operational Risk Management* (July 2026) and is aligned to ISO 22301:2019 *Security and resilience — Business continuity management systems — Requirements*.

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, systems and locations, and to service providers that support critical operations. CPS 230 defines critical operations as processes undertaken by the entity **or its service provider** (para 34), so outsourcing an operation does not take it out of scope.

If [Organisation] is	Business continuity requirements (as at October 2026)
An ADI, general insurer, life company, private health insurer, RSE licensee, or authorised or registered NOHC	CPS 230 paras 33–45 (business continuity), paras 46–61 (service providers) and para 32 (incident notification), determination No. 1 of 2026, in force from 1 July 2026. Foreign ADIs, Category C insurers and EFLICs apply it to their Australian branch operations (para 3). A Head of a group applies it on a group basis (paras 4–5).
An AFS licensee not regulated by APRA	No prescriptive business continuity standard of general application. The <i>Corporations Act 2001</i> requires adequate resources (s912A(1)(d)) and adequate risk management systems (s912A(1)(h)). Adopt this Policy as good practice, scaled to the business.
Another financial services business	Adopt this Policy as good practice, scaled to the nature, size and complexity of the business. ISO 22301 can be used as the reference model and, if wanted, for certification.

CPS 230 replaced the former APRA business continuity standards (CPS 232 and SPS 232) and outsourcing standards. CPS 230 business continuity planning must be consistent with, and not conflict with or undermine, the entity's recovery and exit planning under CPS 190 (CPS 230 para 17).

3. Key definitions

Term	Meaning
Business continuity	The capability of [Organisation] to continue delivering products and services within acceptable timeframes at predefined capacity during a disruption (ISO 22301).
Business continuity management (BCM)	The ongoing program of governance, analysis, planning, testing and improvement described in this Policy. Under ISO 22301 the program is run as a business continuity management system (BCMS).
Disruption	An event, expected or unexpected, that causes an unplanned negative deviation from the expected delivery of products or services. Includes loss of people, premises, technology, data or a service provider.
Critical operation	A process undertaken by [Organisation] or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on depositors, policyholders, beneficiaries or other customers, or on [Organisation] 's role in the financial system (CPS 230 para 34).
Tolerance levels	For each critical operation, the Board-approved limits for (a) the maximum period of disruption , (b) the maximum extent of data loss and (c) the minimum service levels while operating under alternative arrangements (CPS 230 para 37).
Maximum period of disruption	The maximum time [Organisation] would tolerate a disruption to a critical operation before the impact is unacceptable (CPS 230 para 37(a)). CPG 230 Table 4 links it to the maximum allowable disruption and, for information assets, the recovery time objective (RTO).
Maximum data loss	The maximum extent of data loss [Organisation] would accept as a result of a disruption (CPS 230 para 37(b)), usually expressed as a recovery point objective (RPO), the point in time to which data must be recovered.
Minimum service level	The minimum level of service [Organisation] would maintain while operating under alternative arrangements (CPS 230 para 37(c)); CPG 230 calls this the recovery level objective.
Business impact analysis (BIA)	The process of analysing the impact over time of a disruption on the organisation, used to identify critical operations, their dependencies and recovery priorities (ISO 22301; ISO/TS 22317).

Term	Meaning
Business continuity plan (BCP)	The documented plan setting out how [Organisation] would maintain its critical operations within tolerance levels through disruptions (CPS 230 paras 33(c) and 39). [Organisation] may have several BCPs, and a BCP may include separate crisis management and disaster recovery plans (CPS 230 footnote 12).
Disaster recovery plan (DRP)	A plan to recover critical information assets (systems, applications, data and infrastructure). Required for critical information assets as part of the BCP (CPS 230 para 33(c)).
Contingency arrangement	An alternative way to deliver a critical operation (for example a manual process, alternative provider or alternative site) used when the primary recovery plan does not work as intended (CPG 230 para 35).
Severe but plausible scenario	A scenario of extreme but realistic disruption, used for scenario analysis and testing to show whether critical operations can be kept within tolerance (CPS 230 paras 26(c), 42 and 43).
Material service provider	A service provider 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).
Crisis	As defined in the RiskFA Crisis Management Plan: a situation that threatens [Organisation]'s strategic objectives, reputation or viability and needs strategic decisions by senior leaders.
Test / exercise	A test checks whether a specific plan, system or recovery step works (for example a DR failover). An exercise rehearses people in their roles against a scenario (for example a tabletop exercise). Both are part of the testing program (section 18).

4. Principles

1. **Customers and the financial system first.** Critical operations and tolerances are set by the harm a disruption would cause to customers, beneficiaries and the financial system, not only by the cost to [Organisation].
2. **Assume disruption will happen.** Plans are built for the severe but plausible case, not only the likely one.
3. **End to end.** Each critical operation is mapped across every process, system, team, location and service provider it depends on, including fourth parties.
4. **Tolerances are the test.** Recovery capability is measured against Board-approved tolerance levels, and the gap is reported honestly.
5. **Credible, not theoretical.** A plan is credible only when it has the people, resources and technology to run it, and testing shows it works.
6. **Integrated.** Business continuity is part of the risk management framework and is consistent with incident management, cyber response, crisis management and recovery and exit planning.
7. **Clear accountability.** Every critical operation, plan, recovery strategy and action has a named owner.
8. **Learn and improve.** Lessons from tests, real disruptions and audits change the plans, the controls and, where needed, the tolerances.

5. Standards and alignment

This Policy applies the regulatory requirements of CPS 230 and the guidance in CPG 230, and follows the business continuity management lifecycle of the ISO 22300 series:

Source	What it provides	Status as at October 2026
APRA CPS 230 <i>Operational Risk Management</i>	Binding requirements for APRA-regulated entities: critical operations, tolerance levels, BCP content, testing, internal audit, Board reporting and APRA notification (paras 33–45).	Determination No. 1 of 2026 (F2026L00475), in force from 1 July 2026.
APRA CPG 230 <i>Operational Risk Management</i>	APRA's expectations and better practice (paras 15–18 and 30–43, Table 4 tolerance types).	July 2026 edition.

Source	What it provides	Status as at October 2026
ISO 22301:2019 <i>Business continuity management systems — Requirements</i>	The international requirements for a BCMS: context, leadership, planning, support, operation (BIA and risk assessment, strategies and solutions, plans and procedures, exercise programme), evaluation and improvement.	Edition 2, with Amendment 1:2024 (climate action changes).
ISO 22313:2020 <i>Guidance on the use of ISO 22301</i>	Guidance on implementing each ISO 22301 requirement.	Current.
ISO/TS 22317:2021 <i>Guidelines for business impact analysis</i>	Detailed guidance on the BIA process.	Current.
ISO 22361:2022 <i>Crisis management — Guidelines</i>	Guidance on strategic crisis management capability (used by the Crisis Management Plan).	Current.

ISO 22301 is a voluntary standard. [Organisation] [does / does not] seek certification. Meeting ISO 22301 does not on its own show compliance with CPS 230: CPS 230 adds specific requirements, such as Board-approved tolerance levels, the 24-hour APRA notification and an annual business continuity exercise.

6. Governance and the three lines of accountability

CPS 230 makes the Board ultimately accountable for oversight of operational risk management, including business continuity (para 19), and requires clear roles and responsibilities for senior managers (para 20). Senior management must give the Board clear and comprehensive information on the expected impact on critical operations when the Board makes decisions that could affect their resilience (para 22).

Line	Who	Responsibilities
First line	Owners of critical operations, business units, technology, operations, procurement and service provider owners	Own and maintain BIAs, plans, recovery strategies and DR capability; run tests; manage disruptions; keep critical operations within tolerance; raise and fix issues.

Line	Who	Responsibilities
Second line	Risk (including the [Business Continuity Manager] where placed in Risk) and Compliance	Own this Policy and the methodology; challenge critical operation identification, tolerance levels, BIAs and test results; monitor tolerance compliance; assess APRA notification; report to the Board Risk Committee.
Third line	Internal Audit	Periodically review the BCP and give the Board assurance that it is credible and that testing is adequate and has been conducted satisfactorily (CPS 230 para 45).

7. Roles and responsibilities

Role	Responsibilities
Board	Approves this Policy, the BCP and tolerance levels for critical operations; reviews the results of testing and oversees the execution of findings (CPS 230 para 21(b)); receives reports of any failure to meet tolerance levels with a remediation plan (para 40); receives internal audit assurance (para 45).
Board Risk Committee	Recommends the Policy, BCP and tolerances to the Board; oversees the business continuity program, testing program and remediation.
Chief Executive Officer and executive team	Ensure critical operations in their areas can be kept within tolerance; provide resources; lead or take part in the Crisis Management Team and the annual exercise. Where the Board has delegated it, approve more granular plans and tolerance levels that sit beneath, and align to, Board-approved documents (CPG 230 para 13).
Accountable persons (FAR, where applicable)	Meet their obligations for the parts of the business they are responsible for, including the resilience of critical operations in their area. CPG 230 para 18 expects an accountable person to approve any decision not to classify an APRA-listed operation as critical.
[Chief Operating Officer] (business continuity executive)	Accountable for the business continuity program; owns the register of critical operations and the BCP; reports tolerance compliance; decides BCP activation where the Crisis Management Team is not activated.
Chief Risk Officer	Owns this Policy; provides independent challenge of critical operations, tolerances, BIAs and testing; reports to the Board Risk Committee; oversees APRA notification with Compliance.
Chief Technology Officer and Chief Information Security Officer	Own disaster recovery for critical information assets, backup and restoration capability, and the link to the RiskFA Cyber Incident Response Plan; ensure RTOs and RPOs support the tolerance levels.
Head of Compliance / General Counsel	Assess and make APRA notifications under CPS 230 paras 32 and 41 and other regulatory notifications; advise on legal and contractual obligations in a disruption.
[Business Continuity Manager]	Runs the program day to day: methodology, templates, BIA cycle, plan quality, the testing program, training and reporting.

Role	Responsibilities
Critical operation owner	A senior executive accountable for one critical operation end to end: its BIA, tolerance proposal, BCP, recovery strategies, dependencies (including service providers), testing and remediation.
Service provider owner	Ensures each material service provider supporting a critical operation has adequate business continuity arrangements, joins testing where appropriate, and that [Organisation] can execute its BCP if the provider fails (CPS 230 para 55(c)).
All staff	Know their role in the plans that apply to them, keep contact details current, take part in training and exercises, and report disruptions promptly.

8. The business continuity lifecycle

The program runs as a continuous cycle, consistent with ISO 22301 (plan, do, check, act) and the CPS 230 requirements:

Stage	What must happen	Section
1. Identify	Define, identify and maintain the register of critical operations.	9
2. Analyse	Complete a BIA for each critical operation, mapping processes, resources, dependencies and the impact of disruption over time.	10
3. Set tolerances	Set and approve tolerance levels for each critical operation.	11
4. Assess	Assess risks and run scenario analysis; take reasonable steps to minimise the likelihood and impact of disruption.	12
5. Design strategies	Select recovery strategies and contingency arrangements for people, premises, technology, data and service providers.	13–14
6. Plan	Document BCPs, DR plans and the communications strategy; maintain the capability to execute them.	15–17
7. Test	Run the systematic testing program, including the annual business continuity exercise.	18
8. Respond	Activate the BCP when needed; monitor tolerances; notify the Board and APRA; return to normal operations promptly.	16, 19, 20

Stage	What must happen	Section
9. Review and improve	Update plans annually and after changes; fix issues; obtain internal audit assurance.	21–22

9. Identifying critical operations

[Organisation] must define, identify and maintain a **register of critical operations** (CPS 230 para 33(a)). In identifying them, **[Organisation]** focuses on outward-facing services that support customers and the financial system (CPG 230 para 15) and considers operations that, if disrupted beyond tolerance, would have a direct or indirect material adverse impact on customers, or could affect the broader financial system or economy (CPG 230 para 16).

At a minimum, the following must be classified as critical operations unless **[Organisation]** can justify otherwise (CPS 230 para 35):

Entity	Minimum critical operations
ADI	Payments; deposit-taking and management; custody; settlements and clearing
Insurer (general, life, private health)	Claims processing
RSE licensee	Investment management; fund administration
All APRA-regulated entities	Customer enquiries; 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).
- Where **[Organisation]** decides that an operation on APRA's minimum list is not critical, the reasons are documented, approved by an accountable person and reviewed at least annually (CPG 230 para 18).
- APRA may require **[Organisation]** to classify a business operation as critical (CPS 230 para 36).
- The register is reviewed at least **[annually]**, and whenever a new product, service, geography, technology or service provider arrangement is approved (CPS 230 para 25).

The register records for each critical operation at least: its name and description, the accountable owner, the tolerance levels, and the material service provider arrangements that

support it (CPG 230 para 31), together with the date of the last BIA, test and review.

10. Business impact analysis

A BIA is completed for every critical operation, and for other important operations that the [Business Continuity Manager] nominates, using the template in Appendix A. The BIA follows the ISO 22301 requirements for business impact analysis and the guidance in ISO/TS 22317. It must:

- describe the operation end to end, from the customer or beneficiary back through every internal process and service provider;
- identify and document the **processes and resources** needed to deliver the operation: people, technology, information (data), facilities and service providers, the interdependencies across them, and the associated risks, obligations, key data and controls (CPS 230 para 26(b));
- assess the impact of disruption **over time** (for example at [1 hour, 4 hours, 1 day, 3 days, 1 week, 1 month]) across the six RiskFA impact categories: financial; customers; regulatory and legal; operations and critical operations; information security and privacy; and reputation;
- identify the point at which the impact becomes unacceptable, which informs the proposed maximum period of disruption;
- identify the data that must be preserved and how far back it could be reconstructed, which informs the proposed maximum data loss;
- identify the minimum service the operation must deliver under alternative arrangements, and the minimum people and resources needed to deliver it;
- identify peak periods and time-critical dates (for example month end, payroll, rollover dates, claims surges after a natural catastrophe); and
- record single points of failure, key person dependencies and concentration risk (for example several critical operations relying on one data centre, cloud region or provider).

BIAs are refreshed at least every [12 months] and when the operation, its systems or its service providers change materially. Second line reviews and challenges each BIA.

11. Tolerance levels

For each critical operation, [Organisation] must establish tolerance levels for (CPS 230 para 37):

Tolerance	CPS 230 requirement	How it is expressed (CPG 230 Table 4)
Maximum period of disruption	The maximum period of time [Organisation] would tolerate a disruption to the operation (para 37(a))	Maximum allowable disruption, in hours or days, for the operation as a whole. Recovery time objectives (RTOs) for supporting information assets should be shorter.
Maximum data loss	The maximum extent of data loss [Organisation] would accept as a result of a disruption (para 37(b))	Recovery point objective (RPO), in time, informed by how far back data can be reconstructed (for example by re-keying). It drives backup and replication frequency.
Minimum service levels	The minimum service levels [Organisation] would maintain while operating under alternative arrangements (para 37(c))	Recovery level objective: the minimum level of service, volumes or customer outcomes to be maintained, and the minimum people and resources needed.

- Tolerances are proposed by the critical operation owner from the BIA, challenged by second line, recommended by the [Board Risk Committee] and **approved by the Board** (CPS 230 para 21(b)). The Board ensures the BCP aligns with its tolerances (CPG 230 para 10).
- In setting tolerances, [Organisation] considers the impact on customers and other stakeholders, the financial and reputational impact on [Organisation] and the broader financial system (including flow-on effects and contagion), legal and regulatory requirements (including any tolerance set by APRA), and recovery objectives (CPG 230 para 32).
- Tolerances are set from the customer's point of view and apply to the critical operation end to end, including any part performed by a service provider.
- Tolerances must be specific and measurable, so that it is clear during a disruption whether the operation is within or outside tolerance.
- Tolerances are reassessed at least [annually] and as lessons are learned from actual disruptions, testing, scenario analysis and industry practice (CPG 230 para 33). APRA may require tolerances to be reviewed and changed, or may set them (CPS 230 para 38).
- Each critical operation has a tolerance statement using the template in Appendix B.

Tolerance levels are the Board's limits for disruption, not targets. A recovery capability that only just meets the tolerance in testing leaves no margin in a real event. Good practice is to design RTOs and RPOs with a buffer, for example recovering supporting systems within [50–75%] of the maximum period of disruption.

12. Risk assessment, prevention and scenario analysis

[Organisation] must take reasonable steps to minimise the likelihood and impact of disruptions to its critical operations (CPS 230 para 33(b)) and, to the extent practicable, prevent disruption, adapt processes and systems to continue within tolerance, and return to normal operations promptly (para 13). In practice:

- the risks to each critical operation are assessed and rated under the RiskFA Risk Management Framework, and key controls (for example resilience in system design, redundancy, backups, physical security, capacity management, change controls and service provider oversight) are tested for design and operating effectiveness;
- [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));
- the impact on operational resilience of new products, services, geographies, technologies and strategic decisions is assessed before approval (CPS 230 para 25); and
- information and technology capability is maintained to support critical operations, including monitoring the age and health of information assets (CPS 230 para 24).

The scenario library is reviewed at least [annually] by second line and includes, where relevant:

Scenario category	Examples of severe but plausible scenarios
Technology	Prolonged outage of a core system or data centre; failed change; loss of a cloud region; corrupted data replicated to backups
Cyber	Ransomware encrypting production and backup systems; destructive malware; extended denial of service; compromise of identity systems (coordinated with the RiskFA Cyber Incident Response Plan)
Service providers	Sudden failure, insolvency or exit of a material service provider; a cyber incident at a provider; failure of a fourth party that several providers rely on; concentration of providers in one location

Scenario category	Examples of severe but plausible scenarios
People	Pandemic or illness affecting [30–50%] of staff; loss of a key team or key persons; industrial action
Premises and environment	Loss of a main office or operations site; regional natural hazard (flood, bushfire, storm, heatwave) affecting staff and sites at once; utilities or telecommunications outage. Climate-related hazards should be considered (ISO 22301 Amd 1:2024 adds climate change as an issue to consider).
Market and system-wide	Outage of a payment system, exchange or other financial market infrastructure; claims or redemption surge after a catastrophe or market event
Combined	Two or more of the above at once, for example a cyber attack during a natural disaster or peak period

13. Recovery strategies

For each critical operation, the owner selects and documents strategies that will keep the operation within tolerance (ISO 22301 business continuity strategies and solutions). Strategies cover protection before a disruption, continuation during it and recovery after it, and address every resource the operation depends on:

Resource	Strategies to consider	Minimum expectation
People	Cross-training and documented procedures; succession for key roles; split teams across sites; remote working; surge staff or agreed support from other business units or providers	No critical operation depends on a single person; minimum staffing for the minimum service level is identified and can be met.
Premises	Work from home; alternative office or workspace (owned, shared or provided); split operations across sites	Staff for each critical operation can work from at least one alternative location within the maximum period of disruption.
Technology	Resilient design (redundancy, active-active or failover); disaster recovery sites or cloud regions; tested DR plans; capacity for recovery	DR plans exist for critical information assets (CPS 230 para 33(c)); RTOs support the maximum period of disruption.

Resource	Strategies to consider	Minimum expectation
Data and information	Backups and replication in line with the RPO; immutable or offline backups to protect against ransomware; tested restoration; ability to reconcile and re-key	Backups meet the maximum data loss tolerance and restoration is tested at least [annually] for each critical operation.
Service providers and fourth parties	Provider BCP and DR requirements in contracts; joint testing; alternative or substitute providers; ability to bring services in-house; exit plans	[Organisation] can execute its BCP if a material service provider fails (CPS 230 para 55(c)).
Manual and contingency arrangements	Manual workarounds, alternative channels, prioritising the most vulnerable customers, temporary product or service changes	Contingency arrangements exist where the primary recovery plan may not work as intended (CPG 230 para 35).

Strategies must be credible: **[Organisation]** must maintain the capabilities required to execute the BCP, including access to people, resources and technology. These capabilities may be held internally or through an agreement with another party, which must then meet CPS 230's service provider requirements (CPS 230 para 40 and footnote 13).

14. Material service providers and fourth parties

Many critical operations depend on service providers. This Policy works with the **[Service Provider Management Policy]** required by CPS 230 paras 46–47.

- The register of material service providers (CPS 230 para 48) is linked to the register of critical operations, so that the providers that each critical operation depends on are known.
- Before entering into or materially changing a material arrangement, **[Organisation]** assesses the provider's ability to provide the service on an ongoing basis, including its business continuity arrangements and geographic or concentration risk (CPS 230 para 52).
- Formal agreements include a force majeure provision stating which parts of the contract continue in a force majeure event (CPS 230 para 53(f)) and should set out the provider's BCP and DR obligations, recovery times consistent with **[Organisation]**'s tolerance levels, notification of disruptions within **[2–4 hours]**, and the right to receive test results and join tests.
- For each material arrangement, **[Organisation]** must ensure it can execute its BCP if needed and can conduct an orderly exit (CPS 230 para 55(c) and (d)).

- **[Organisation]** seeks to confirm that material service providers maintain robust BCP testing, and considers joint testing (CPG 230 para 39). The testing program includes disruptions to services provided by material service providers (CPS 230 para 43).
- The **[Service Provider Management Policy]** covers the risks from fourth parties that material service providers rely on to deliver a critical operation (CPS 230 para 47(c)). Business continuity analysis considers these dependencies.

15. Business continuity plan content

[Organisation] must maintain a **credible BCP** that sets out how it would maintain its critical operations within tolerance levels through disruptions, including disaster recovery planning for critical information assets (CPS 230 para 33(c)). **[Organisation]** may have one BCP or several (for example by business unit or critical operation), and may keep separate crisis management and disaster recovery plans (footnote 12). The plans should be clearly linked to each other (CPG 230 para 36). As a minimum the BCP must include (CPS 230 para 39):

CPS 230 para 39	Required content
(a)	The register of critical operations and associated tolerance levels.
(b)	Triggers to identify a disruption and prompt activation of the plan, and arrangements to direct resources in the event of activation.
(c)	The actions [Organisation] would take to maintain its critical operations within tolerance levels through disruptions.
(d)	An assessment of the execution risks, required resources and preparatory measures, including key internal and external dependencies needed to support effective implementation of the BCP actions.
(e)	A communications strategy to support execution of the plan.

CPG 230 para 34 expects the BCP to cater for all stages of a disruption: triggers and identification, initial actions (such as alternative arrangements), further actions, assessment and communications. Appendix C is the BCP content checklist. Plans must be written so that a capable deputy who has not written them can follow them.

16. Activation, response and the link to crisis management

[Organisation] must activate its BCP if needed in the event of a disruption (CPS 230 para 33(d)).

- **Triggers.** Each BCP sets clear triggers, for example: a critical operation is disrupted or likely to be disrupted for more than [50%] of its maximum period of disruption; data loss approaching the maximum data loss tolerance; loss of a site, a key system or a material service provider; or a forecast event (such as a severe weather warning) likely to cause disruption.
- **Authority.** The critical operation owner, the [Chief Operating Officer] or their deputies may activate a BCP. Activation does not need to wait for the full facts: activate early and stand down if the disruption is contained.
- **Incident management.** Every disruption is recorded, rated and escalated as an incident under the RiskFA Incident & Issues Management Standard. A disruption to a critical operation within tolerance is rated at least High; one outside tolerance is rated Critical.
- **Crisis management.** A disruption to a critical operation outside tolerance (a Critical incident) activates the Crisis Management Team under the RiskFA Crisis Management Plan, as every Critical incident does under the RiskFA Incident & Issues Management Standard; a disruption likely to go outside tolerance may activate it. The Crisis Management Team makes the strategic decisions; BCP teams run the recovery of each critical operation.
- **Cyber.** Where the cause is a cyber security incident, the RiskFA Cyber Incident Response Plan runs the technical response, and the BCP keeps critical operations going. Recovery from a cyber incident must not restore compromised systems or data before the incident response team agrees it is safe.
- **Tolerance clock.** From the start of a disruption, the critical operation owner records the time and tracks the disruption against each tolerance level (section 19).

17. Communications

The BCP's communications strategy (CPS 230 para 39(e)) is consistent with the RiskFA Crisis Management Plan and covers:

- who is told, by whom, how and when: staff, customers and beneficiaries, material service providers, regulators, the Board, intermediaries and, where relevant, the media and the market;
- pre-approved templates and holding statements for likely scenarios, including customer messages about alternative ways to get service;
- out-of-band channels (for example a mass notification tool, personal mobile phones and an offline contact list) that do not rely on systems that may be disrupted;
- support for vulnerable customers and customers in financial hardship during the disruption; and

- approval of all external communications by [CEO / Head of Communications / General Counsel].

18. Testing and exercise program

[Organisation] must have a **systematic testing program** for its BCP that covers all critical operations and includes an **annual business continuity exercise**. The program must test the effectiveness of the BCP and [Organisation]'s ability to meet tolerance levels in a range of severe but plausible scenarios (CPS 230 para 42). It must be tailored to [Organisation]'s material risks and include disruptions to services provided by material service providers and scenarios where contingency arrangements are required (para 43). APRA may require an APRA-determined scenario to be included (para 43).

Test or exercise type	Purpose	Minimum frequency
Plan walkthrough	Owners and teams check the plan is accurate, current and understood	Each plan, at least [annually]
Contact and notification test	Check call trees and mass notification work and contact details are current	At least [twice a year]
Tabletop exercise	Teams discuss their response to a scenario, step by step, and test decisions and communications	Each critical operation, at least [annually]
Technical recovery test (DR failover, backup restoration)	Prove systems and data can be recovered within RTO and RPO, and that recovered systems work for the business	Each critical information asset, at least [annually]
Alternative site or work-from-home test	Prove staff can deliver the minimum service level from the alternative arrangements	Each critical operation, at least [every 2 years]
Contingency arrangement test	Prove manual workarounds or alternative providers work at the volumes needed	Each contingency arrangement, at least [every 2 years]
Material service provider test	Joint or provider-led test of the provider's recovery and [Organisation]'s ability to execute its BCP if the provider fails	Each material service provider supporting a critical operation, within the [3-year] cycle

Test or exercise type	Purpose	Minimum frequency
Annual business continuity exercise	A severe but plausible scenario that tests the ability to keep several critical operations within tolerance, with the Crisis Management Team taking part	At least annually (CPS 230 para 42)

- All critical operations are tested within a multi-year cycle of no more than **[3 years]** (CPG 230 para 37), with higher-risk operations tested more often.
- Tests should be realistic and should measure results against each tolerance level, not just whether a step was completed. Testing only the easy case does not show the plan is credible.
- The annual testing schedule is approved by the **[Board Risk Committee]** at the start of each year.
- Each test produces a report using Appendix D, covering the scope (including the critical operations and tolerance levels tested and excluded), what was demonstrated (including whether tolerance levels were met), and the issues, root causes and remediation with owners and due dates (CPG 230 para 38).
- Issues are recorded and tracked under the RiskFA Incident & Issues Management Standard. Test results and the execution of findings are reported to and reviewed by the Board (CPS 230 para 21(b); CPG 230 para 38).
- Where scenarios overlap, exercises are coordinated with cyber incident response testing (CPS 234 para 26) and recovery and exit plan testing.

19. Monitoring tolerance, Board reporting and APRA notification

[Organisation] must monitor compliance with its tolerance levels and report any failure to meet them, together with a remediation plan, to the Board (CPS 230 para 40).

Situation	Who is told	When
Disruption to a critical operation, any length	Critical operation owner, [COO] , CRO	Immediately; recorded as an incident
Disruption likely to exceed [50%] of the maximum period of disruption, or approaching any tolerance	CEO, CRO, General Counsel; Crisis Management Team considered	Within [1 hour]

Situation	Who is told	When
Disruption to a critical operation outside tolerance	APRA (CPS 230 para 41)	As soon as possible and not later than 24 hours after suffering the disruption
Failure to meet a tolerance level (in a real disruption)	Board, with a remediation plan (CPS 230 para 40)	Board Risk Committee chair within [24 hours]; full Board at its next meeting or sooner as the chair directs
Operational risk incident likely to have a material financial impact or a material impact on the ability to maintain critical operations	APRA (CPS 230 para 32). An incident already notified under CPS 234 need not be notified again (footnote 11).	As soon as possible and not later than 72 hours after becoming aware
Information security incident that materially affected, or could have materially affected, [Organisation] or its customers, or that has been notified to another regulator (CPS 234 para 35)	APRA	As soon as possible and not later than 72 hours after becoming aware
Test shows a tolerance level cannot be met	Board Risk Committee; reported to the Board with the remediation plan	Next scheduled report, or sooner if the gap is significant

- The APRA notification under para 41 must cover the nature of the disruption, the action taken, the likely impact on [Organisation] 's business operations and the timeframe for returning to normal operations. APRA notifications are made electronically using the form on APRA's website (CPG 230 para 14).
- [Head of Compliance] decides and records whether each notification is required. The 24-hour clock starts when the disruption goes outside tolerance. Do not wait for the disruption to end before notifying.
- Other notifications (for example ASIC, the OAIC, ASD under the SOCI Act, AUSTRAC or ASX) are assessed under the RiskFA Incident & Issues Management Standard and the RiskFA Crisis Management Plan.

20. Returning to normal operations

[Organisation] must return to normal operations promptly after a disruption is over (CPS 230 para 33(e)). Each BCP sets out how to:

- confirm the cause is resolved and that it is safe to return (for a cyber incident, with the incident response team's agreement);
- move back from alternative arrangements in a controlled way, including reconciling, validating and re-keying data, and clearing backlogs;
- confirm that customers affected by the disruption are identified and, where they have suffered loss, remediated under the RiskFA Incident & Issues Management Standard;
- stand down teams formally and record the time of return to normal operations; and
- complete a post-incident review for every disruption to a critical operation outside tolerance, and for others at the CRO's discretion, with lessons fed into the BCP, the BIA, the tolerances and the testing program.

21. Plan maintenance and review

- [Organisation] must update its BCP, as necessary, on an **annual basis** to reflect any changes in legal or organisational structure, business mix, strategy or risk profile, or shortcomings identified through review and testing (CPS 230 para 44). CPG 230 para 40 also expects an update as soon as possible after a material change, such as a merger, acquisition or major external shock.
- BCPs are updated using the results of testing, internal audit findings and lessons from actual disruptions (CPG 230 para 41).
- Contact lists and call trees are checked at least [quarterly].
- Each plan shows its version, owner, date of last review and date of last test. Superseded versions are withdrawn, and current printed or offline copies are held by key people.
- Business continuity is included in the required reviews of operational risk management under CPS 220 / SPS 220 (CPS 230 para 16).
- Changes to critical operations, systems, premises or service providers go through the change and new product approval processes, which must assess the impact on the BCP and tolerances.

22. Internal audit and assurance

[Organisation] 's internal audit function must periodically review the BCP and provide assurance to the Board that the BCP sets out a credible plan for how [Organisation] would maintain its critical operations within tolerance levels through severe disruptions, and that testing procedures are adequate and have been conducted satisfactorily (CPS 230 para 45).

- Internal Audit reviews business continuity at least every [2–3 years], with the audit program assessing all aspects of business continuity capability over time (CPG 230 para 43).
- Additional reviews may be triggered by changes to services, processes, information assets, the business environment or stakeholder expectations (CPG 230 para 43).
- The Board may seek assurance from expert opinion or other means to complement internal audit (CPG 230 para 42).
- Second line reviews a sample of BIAs, plans and test reports each year and reports the results to the [Board Risk Committee].

23. Training and awareness

- All staff receive business continuity awareness at induction and [annually]: what to do in a disruption, how they will be contacted and where to find information.
- People with a role in a BCP or DR plan, and their deputies, are trained in that role before they rely on it, and take part in at least one exercise each [year].
- Members of the Crisis Management Team and their deputies are trained under the RiskFA Crisis Management Plan.
- Board members receive a briefing on critical operations, tolerances and the testing program at least [annually], and should take part in the annual business continuity exercise where a Board decision is part of the scenario.

24. Reporting and measures

Second line reports to the executive [quarterly] and to the [Board Risk Committee] at least [half-yearly] on:

- the register of critical operations and any changes, and tolerance levels for Board approval;
- disruptions to critical operations, performance against tolerance and any APRA notifications;
- results of tests and exercises, whether tolerances were met, and the execution of

findings;

- critical operations whose recovery capability does not yet meet tolerance, with the remediation plan and interim measures;
- open business continuity issues and overdue actions; and
- the status of material service provider business continuity and testing.

Measure	Typical target
Critical operations with a current BIA (within [12 months])	[100%]
Critical operations with Board-approved tolerance levels	[100%]
Critical operations tested within the cycle	[100%] within [3 years] ; [100%] of high-risk operations [annually]
Tests in which all tolerance levels were met	Trending up; every failure has a remediation plan
BCPs reviewed and updated within [12 months]	[100%]
Business continuity actions overdue	≤ [5–10%] ; no High or Critical action more than [90 days] overdue
Material service providers supporting critical operations with evidence of tested BCP and DR	[100%]

These targets are common industry practice, not regulatory requirements. Set your own in line with your risk appetite.

25. Accountability and compliance with this Policy

Breaches of this Policy, including failing to maintain or test a plan, or delaying the escalation of a disruption, are managed under the RiskFA Incident & Issues Management Standard and the RiskFA Consequence Management Framework, and are considered in performance and variable remuneration outcomes under the RiskFA Remuneration Policy (CPS 511 where it applies). Exemptions need the written approval of the CRO, with reasons and an expiry date, and are reported to the [Board Risk Committee] . No exemption may be granted from a requirement of CPS 230.

26. Related documents

- The RiskFA Risk Management Framework, Risk Appetite Statement and Incident & Issues Management Standard
- The RiskFA Crisis Management Plan, Cyber Incident Response Plan, Cyber Security Policy and Data Breach Response Plan
- The RiskFA Operational Risk Management Policy, [Service Provider Management Policy] , [Recovery and Exit Plan] (CPS 190, where it applies), [Business Continuity Plans] , [Disaster Recovery Plans] , [Pandemic Plan]
- APRA: CPS 230 *Operational Risk Management* (2026) and CPG 230 (July 2026); CPS 234 *Information Security* and CPG 234; CPS 190 *Recovery and Exit Planning*; CPS 900 *Resolution Planning*
- Standards: ISO 22301:2019 *Business continuity management systems — Requirements* (and Amd 1:2024); ISO 22313:2020 *Guidance on the use of ISO 22301*; ISO/TS 22317:2021 *Guidelines for business impact analysis*; ISO 22361:2022 *Crisis management — Guidelines*; AS ISO 31000 *Risk management*

Appendix A. Business impact analysis template

Complete one BIA for each critical operation. Attach process maps and dependency diagrams.

Section	Content
1. Operation	Name, description, accountable owner, business unit; why it is (or is not) a critical operation; CPS 230 para 35 category if any.
2. Customers and stakeholders	Who relies on it (customer segments, vulnerable customers, beneficiaries, intermediaries, other financial institutions, market infrastructure); volumes and values per day.
3. End-to-end process	Main process steps from the customer back to settlement or completion; which steps are performed by service providers.
4. Peak periods	Times of day, days of month and seasons when a disruption would be worse; time-critical dates.
5. Impact over time	Rate the impact at [1 hour, 4 hours, 1 day, 3 days, 1 week, 1 month] in each impact category (table below).

Impact category	1 hour	4 hours	1 day	3 days	1 week	1 month
Reputation	[]	[]	[]	[]	[]	[]
Overall (highest)	[]	[]	[]	[]	[]	[]

Rate each cell Critical, High, Medium or Low using the RiskFA rating scale. The point where the overall rating first reaches Critical is a strong indicator of the maximum period of disruption.

Appendix B. Critical operation tolerance statement template

Item	Detail
Critical operation	[Name] ; [register ID]
Description	[What the operation delivers, to whom, and in what volumes]
Accountable owner and deputy	[Name, role] ; [Name, role]
Reason for classification	[CPS 230 para 35 minimum list / BIA outcome / CPS 900 critical function / APRA requirement]
Maximum period of disruption	[for example 4 hours] measured from [the time the operation is first unavailable to customers]
Maximum data loss	[for example no loss of completed transactions; up to 15 minutes of in-progress data that can be re-keyed]
Minimum service levels under alternative arrangements	[for example 80% of normal daily payment volumes; urgent claims paid within 2 business days; customer enquiry line answering within 10 minutes]
Basis for the tolerances	[Summary of BIA impact over time; customer, financial system, legal and regulatory considerations (CPG 230 para 32)]
Supporting RTOs and RPOs	[Key systems and their RTO / RPO, each inside the tolerance]
Material service providers	[Providers and their committed recovery times]
Current capability	[Meets tolerance / does not meet tolerance] , as shown by [test, date]
Gaps and remediation	[Actions, owners, due dates; interim measures]
Measurement during a disruption	[How the start time, data loss and service levels are measured and by whom]
Approval	Recommended by [Board Risk Committee] on [date] ; approved by [Board] on [date] ; next review [date]

Appendix C. BCP content checklist

#	Content	Source	Included
1	Register of critical operations and associated tolerance levels	CPS 230 para 39(a)	☐
2	Triggers to identify a disruption and prompt activation of the plan	CPS 230 para 39(b)	☐
3	Activation authority, deputies and arrangements to direct resources	CPS 230 para 39(b)	☐
4	Actions to maintain each critical operation within tolerance levels, by stage: initial actions, further actions, assessment	CPS 230 para 39(c); CPG 230 para 34	☐
5	Contingency arrangements where recovery plans may not work as intended	CPG 230 para 35	☐
6	Assessment of execution risks, required resources and preparatory measures	CPS 230 para 39(d)	☐
7	Key internal and external dependencies, including material service providers and fourth parties	CPS 230 paras 39(d), 26(b)	☐
8	Disaster recovery plans for critical information assets, with RTOs and RPOs	CPS 230 para 33(c)	☐
9	Communications strategy, templates and out-of-band channels	CPS 230 para 39(e)	☐
10	Links to the Crisis Management Plan, Cyber Incident Response Plan, Data Breach Response Plan and Recovery and Exit Plan	CPG 230 para 36; CPS 230 para 17	☐
11	Tolerance monitoring and the process for Board reporting and the 24-hour APRA notification	CPS 230 paras 40, 41	☐
12	Return to normal operations: validation, reconciliation, backlogs, stand-down	CPS 230 para 33(e)	☐
13	Team members, deputies and contact details (including offline copy)	Good practice; ISO 22301	☐

#	Content	Source	Included
14	Customer protection: vulnerable customers, hardship, remediation	Good practice	[]
15	Version, owner, approval, date of last review and last test	CPS 230 para 44	[]

Appendix D. Test and exercise report template

Section	Content
1. Summary	Test or exercise type, date, scenario in two or three sentences, overall result.
2. Scope	Critical operations, systems, sites and service providers included and excluded ; the tolerance levels tested (CPG 230 para 38(a)).
3. Objectives	What the test set out to show, for example 'recover payments processing at the alternative site within 4 hours with no loss of completed transactions'.
4. Scenario	Severe but plausible scenario used, and why; whether it included a material service provider disruption or contingency arrangements (CPS 230 para 43); any APRA-determined scenario.
5. Participants	Teams, executives, Crisis Management Team, Board members, service providers; observers and facilitators.
6. Results against tolerance	For each critical operation: time to recover against the maximum period of disruption; data loss against the maximum data loss; service achieved against the minimum service level. State clearly whether each tolerance level was met (CPG 230 para 38(b)).
7. What worked	Strengths to keep.
8. Issues and root causes	Each issue, its rating and root cause (RiskFA Incident & Issues Management Standard).
9. Actions	Remediation actions, owners and due dates (CPG 230 para 38(c)); changes to the BCP, BIA, tolerances or the testing program.
10. Sign-off and reporting	Critical operation owner, [Business Continuity Manager] , second line reviewer; reported to the [Board Risk Committee] and Board on [date] .

Appendix E. Map to CPS 230 business continuity requirements

CPS 230 para	Requirement (summary)	Policy section
11(b), 13	Maintain critical operations within tolerance through severe disruptions; prevent, adapt and return to normal	1, 12, 20
15(e)	BCPs as part of the risk management framework, regularly tested with severe but plausible scenarios	15, 18
16, 17	Review of operational risk management; consistency with recovery and exit planning	2, 21
19–22	Board accountability and approvals; senior manager roles; information to the Board	6, 7
26(b), 26(c)	Map processes and resources for critical operations; scenario analysis	10, 12
32	Notify APRA of material operational risk incidents within 72 hours	19
33	Register of critical operations; minimise disruption; credible BCP including DR; activate; return to normal	9, 12, 15, 16, 20
34–36	Definition and minimum list of critical operations; APRA may require classification	3, 9
37, 38	Tolerance levels: maximum period, maximum data loss, minimum service levels; APRA may require change	11, Appendix B
39	BCP content	15, Appendix C
40	Capabilities to execute the BCP; monitor tolerance; report failures with a remediation plan to the Board	13, 19
41	Notify APRA within 24 hours of a disruption to a critical operation outside tolerance	19
42, 43	Systematic testing program, annual exercise, severe but plausible scenarios including material service providers	18, Appendix D
44	Update the BCP annually as necessary	21

CPS 230		
para	Requirement (summary)	Policy section
45	Internal audit review and assurance to the Board	22
48, 53(f), 55(c)	Material service providers; force majeure; ability to execute the BCP	14



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

Disclaimer

© 2026 Risk Frameworks Australia

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