

Crisis Management Plan

How to recognise a crisis, activate and run the Crisis Management Team, make and record decisions, communicate with customers, staff, regulators and the media, and recover and learn. 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 plan. 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, names, deputies and contact numbers, set the timeframes to match your size and risk appetite, delete obligations that do not apply to you, and approve the Plan through your governance process. Keep printed and offline copies: in a crisis your offices, systems, email and document stores 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	Crisis Management Plan
Organisation	[Organisation name]
Document owner	[Chief Risk Officer] (or [Chief Operating Officer])
Approved by	[Board] , on the recommendation of the [Board Risk Committee] . Where this Plan forms part of the business continuity plan, the Board approves it under CPS 230 para 21(b)
Version / date approved	[1.0] / [date]
Review cycle	At least [annually] , after every activation of the Crisis Management Team, after the annual business continuity exercise, and after any material change in structure, leadership, regulation or risk profile
Parent documents	The RiskFA Business Continuity Policy; the RiskFA Incident & Issues Management Standard
Offline copies held by	[All Crisis Management Team members and deputies, Board Chair, Company Secretary, Head of Communications]

1. Purpose

This Plan sets out how [Organisation] recognises, responds to and recovers from a **crisis**: a situation serious enough to need strategic decisions by its most senior leaders. It ensures that:

- a crisis is recognised early and the right leaders are brought together quickly, with clear authority;
- people's safety and welfare come first;
- decisions are made on the best available information, recorded, and reviewed as the situation changes;
- customers, staff, regulators, the Board and other stakeholders get timely, accurate and consistent information;
- regulatory notifications are made within the required timeframes;
- critical operations are kept within tolerance, working with the business continuity and incident response plans; and

- [Organisation] learns from every crisis and exercise.

Under APRA Prudential Standard CPS 230 *Operational Risk Management* (2026), a business continuity plan may include separate crisis management plans (footnote 12), and APRA's guidance notes that alignment of business continuity plans with crisis management governance, triggers, actions and communication plans is important (CPG 230 para 36). This Plan follows the guidance in ISO 22361:2022 *Security and resilience — Crisis management — Guidelines*.

2. Scope

This Plan applies to [Organisation] and its subsidiaries, all locations, and any event, whatever its cause, that meets the activation criteria in section 8. This includes events that start at a material service provider or elsewhere in the financial system. The Plan covers the **strategic** response. Operational and technical responses are run under the plans listed in section 3.

3. Relationship to other documents

Document	How it links to this Plan
RiskFA Incident & Issues Management Standard	Every crisis is also an incident. It is recorded, rated, escalated, investigated and closed under that Standard. Critical incidents activate the Crisis Management Team (Standard section 7, stage 2).
RiskFA Business Continuity Policy and [Business Continuity Plans]	Business continuity teams keep critical operations within tolerance. A disruption to a critical operation outside tolerance is a Critical incident and activates the Crisis Management Team; one likely to go outside tolerance may activate it (Policy section 16).
RiskFA Cyber Incident Response Plan	The Cyber Incident Response Team runs the technical response. Critical cyber incidents activate the Crisis Management Team, which takes the strategic decisions, including any decision about extortion.
RiskFA Data Breach Response Plan	The data breach response team runs the containment, assessment and notification of data breaches. Critical breaches activate the Crisis Management Team.
[Disaster Recovery Plans]	Technology teams recover systems and data. The Crisis Management Team sets recovery priorities when there is conflict.
[Recovery and Exit Plan] (CPS 190, where it applies) and [Liquidity Contingency Plan]	Used where a crisis threatens [Organisation] 's financial position. Crisis decisions must be consistent with these plans (CPS 230 para 17).
[Emergency Response Procedures]	Site-level evacuation, shelter and first aid for immediate threats to life. They always come first.
[Media and Communications Policy] , [Continuous Disclosure Policy]	Set who may speak for [Organisation] and how market-sensitive information is handled.

4. Key definitions

Term	Meaning
Incident	As defined in the RiskFA Incident & Issues Management Standard: an event that has caused, or could have caused, a loss, harm, disruption, breach or other adverse outcome.
Critical incident	An incident rated Critical under the RiskFA rating scale, on the highest of the six impact categories.
Crisis	An abnormal and unstable situation that threatens [Organisation] 's strategic objectives, reputation or viability, or the safety of its people, and that needs strategic decisions by senior leaders beyond normal incident management. Crises are often uncertain, fast-moving and highly visible, and may have no ready-made plan.
Emergency	A sudden, urgent event that threatens life, health, property or the environment and needs immediate action (for example fire, flood, a threat of violence). Emergency procedures come before this Plan.
Disruption	As defined in the RiskFA Business Continuity Policy: an unplanned negative deviation from the expected delivery of products or services.
Crisis Management Team (CMT)	The senior team that leads [Organisation] 's strategic response to a crisis (section 10).
Response teams	The operational and technical teams that act under the CMT's direction: business continuity teams, the Cyber Incident Response Team, the data breach response team, technology recovery teams and site emergency teams.
Activation	The formal decision, recorded with the time, to bring the CMT together under this Plan.
Situation report (sitrep)	A short, regular written summary of what is known, what is not known, the impact, the actions under way and the decisions needed.
Decision log	The formal record of every CMT decision, the information it was based on, the options considered, the reasons, the owner and the time (Appendix C).
Holding statement	A short, pre-approved public statement used early in a crisis, before full facts are known (Appendix D).

Term	Meaning
Stand-down	The formal decision, recorded with the time, that the crisis phase is over and remaining work moves to normal management.

5. Principles

1. **People first.** The safety and welfare of staff, customers and the public come before everything else.
2. **Activate early.** It is better to bring the CMT together and stand it down than to activate too late. Activation is never a sign of failure.
3. **Strategic, not operational.** The CMT sets objectives, priorities and boundaries and makes the big decisions. Response teams do the work. The CMT should not try to run the technical response.
4. **Decide with what you know.** Crises rarely give complete information. The CMT makes the best decision available, records its reasons, and reviews the decision when new information arrives.
5. **One version of the truth.** One situation picture, one decision log, one approved set of messages.
6. **Customers and the vulnerable.** Decisions consider their effect on customers and beneficiaries, especially vulnerable customers, as well as on [Organisation].
7. **Meet the clock.** Regulatory notification deadlines run from when [Organisation] becomes aware or suffers the disruption, not from when the crisis ends.
8. **Communicate early, honestly and often.** Say what is known, what is not known and when the next update will be. Never speculate or mislead.
9. **Learn.** Every activation and exercise is reviewed and the lessons are acted on.

6. Standards and good practice

This Plan follows ISO 22361:2022, which gives guidance on planning, establishing, maintaining, reviewing and continually improving a strategic crisis management capability. It covers the context, core concepts, principles and challenges of crisis management; developing a crisis management capability; crisis leadership; the decision-making challenges facing a crisis team; crisis communication; and training, validation and learning from crises. A related standard is ISO 22301:2019, whose requirements for business continuity plans and procedures include a response structure, warning and communication.

ISO 22361 is guidance, not a set of certifiable requirements. The regulatory requirements that

apply to crisis response in Australian financial services are those for business continuity, incident notification and communications summarised in sections 17 and 18.

7. Incidents, crises and response levels

Most incidents are managed by the business under the RiskFA Incident & Issues Management Standard and never become a crisis. The response is organised in three levels:

Level	Typical situation	Who leads	Focus
Operational	Low, Medium or High incident; disruption within tolerance and contained	Incident owner, business continuity team, Cyber Incident Response Team	Contain, fix, recover; record and escalate under the Standard
Tactical	High or Critical incident affecting several teams or a critical operation; coordination needed	Incident Executive or [Chief Operating Officer] , with an incident management team	Coordinate response teams; track tolerances; prepare options and information for the CMT
Strategic (crisis)	Meets one or more activation criteria in section 8	Crisis Management Team, chaired by the [CEO]	Objectives, priorities, major decisions, stakeholders, regulators, Board, reputation

The difference between a Critical incident and a crisis is the need for strategic leadership. Every crisis is a Critical incident, and every Critical incident activates the CMT (RiskFA Incident & Issues Management Standard section 7). Where, after the first meeting, the CMT Chair judges that strategic leadership is not needed, the CMT is stood down and the incident continues at the tactical level; the decision and reasons are recorded.

8. Activation criteria

The CMT must be considered, and should be activated, when any of the following apply or are reasonably likely:

- death, serious injury or a continuing threat to the safety of staff, customers or the public connected with [Organisation] ;
- a critical operation is disrupted outside its tolerance levels, or is likely to be, or several

critical operations are disrupted at once;

- a Critical incident under the RiskFA rating scale in any impact category (always activates the CMT: section 7);
- a cyber security incident that the Cyber Incident Response Plan classifies as Critical, including ransomware or an extortion demand;
- a large-scale data breach or a likely eligible data breach affecting many individuals or sensitive information;
- loss of a main site, region or material service provider with no quick recovery;
- a threat to [Organisation]'s financial soundness, liquidity, capital or solvency, or a market or system-wide event (for example failure of a payment system or financial market infrastructure);
- serious misconduct, fraud or allegations involving the Board or senior executives;
- regulator, law enforcement or government action with major consequences, or a matter likely to require ASX disclosure;
- sustained national media or social media attention, or loss of confidence by customers, investors or partners; or
- any other situation that the [CEO] or [CRO] judges needs strategic leadership.

Do not wait for certainty. If you are unsure whether a situation is a crisis, escalate to the CMT Chair or the [Crisis Management Coordinator] straight away.

9. Activation authority and process

Step	What happens	Who	Target time
1. Escalate	Anyone who believes a situation may meet the criteria in section 8 tells the Incident Executive, [COO], [CRO] or the [Crisis Management Coordinator] immediately, by phone.	Anyone	Immediately
2. Assess	A short call to confirm the facts known, the potential impact and the activation criteria met.	[Crisis Management Coordinator] with the Incident Executive	Within [30 minutes] of escalation
3. Decide	Decision to activate the CMT, put it on standby, or not activate. Recorded with the time and reasons.	Activation authority: [CEO]; or, if unavailable, [CRO], [COO] or [CFO] (any one)	Within [30 minutes] of escalation
4. Notify	CMT members and deputies are called in using the mass notification tool and phone call tree. The first meeting time and channel are set.	[Crisis Management Coordinator]	Within [15 minutes] of the decision
5. Convene	First CMT meeting (in person, at the crisis room or on the out-of-band bridge).	CMT Chair	Within [1 hour] of activation
6. Inform the Board	The Board Chair and [Board Risk Committee] chair are told that the CMT has been activated.	CMT Chair	Within [2 hours] of activation

Any CMT member may put the CMT on **standby** (members told and ready) without full activation. If the activation authorities cannot be reached within [30 minutes], the most senior executive available may activate the CMT and must record the decision.

10. Crisis Management Team roles and deputies

Each role has a named primary and at least one deputy who is trained and has the authority to act. The CMT should be small enough to decide quickly: other people attend when needed.

Role	Primary	Deputy	Responsibilities
------	---------	--------	------------------

Role	Primary	Deputy	Responsibilities
CMT Chair	[CEO]	[COO] / [CRO]	Leads the CMT; sets strategic objectives and priorities; makes final decisions; principal link to the Board Chair; usually the main spokesperson for major announcements.
Crisis Management Coordinator	[Head of Business Continuity / Resilience]	[Name]	Runs the CMT process: calls meetings, sets the agenda (Appendix B), keeps the action list, makes sure the decision log is maintained, sets the meeting rhythm; manages the crisis room and logistics.
Operations and business continuity lead	[Chief Operating Officer]	[Name]	Status of critical operations against tolerance; business continuity activation and recovery; options and resource needs.
Risk lead	[Chief Risk Officer]	[Name]	Independent view of risk; impact against risk appetite and the rating scale; links to incident management; tolerance and notification tracking with Compliance.
Legal and regulatory lead	[General Counsel / Head of Compliance]	[Name]	Legal advice and privilege; regulatory notifications and regulator liaison (section 18); insurer notification; continuous disclosure advice with the Company Secretary.
Technology and security lead	[Chief Technology Officer] / [CISO]	[Name]	Status of systems and data; link to the Cyber Incident Response Team and DR teams; technical options and risks.
Communications lead	[Head of Communications]	[Name]	Communications strategy; drafts all external and internal messages (section 16); media monitoring; spokesperson preparation.
People lead	[Chief People Officer]	[Name]	Staff safety, welfare and accounting for staff; employee assistance; WHS obligations; workforce availability (section 19).

Role	Primary	Deputy	Responsibilities
Customer lead	[Chief Customer Officer]	[Name]	Customer impact, including vulnerable customers and hardship; contact centre and complaints capacity; customer messages and remediation.
Finance lead	[Chief Financial Officer]	[Name]	Financial impact, liquidity and capital; emergency spending authority; insurance claims; market and investor matters with the Company Secretary.
Loggist	[Trained executive assistant]	[Name]	Keeps the decision log and the meeting record in real time (section 14).
Advisers (as needed)	[Company Secretary] , [Head of Internal Audit (observer)] , external legal, crisis communications, forensic or other specialists		Attend at the Chair's invitation. External advisers are engaged through Legal where privilege may matter.

Delegated authority during a crisis: the CMT Chair may approve spending of up to [\$X] and actions outside normal delegations where needed to protect people, customers or critical operations, reporting them to the Board at the next update. Decisions reserved to the Board (for example any ransom or extortion payment, as set out in the RiskFA Cyber Incident Response Plan) stay with the Board.

11. Crisis room and out-of-band communications

- **Primary crisis room:** [location] , with [screens, phones, printed plans and contact lists, whiteboards] .
- **Alternative crisis room:** [second site or a virtual room] , in a different location from the primary.
- **Out-of-band bridge:** [dial-in number / alternative meeting platform] that does not rely on [Organisation] 's main systems, with a backup number. Use it whenever normal systems may be compromised or unavailable, and always when a cyber attacker may be watching email or chat.
- **Mass notification tool:** [name] , with contact details for all staff, kept current [quarterly] .
- **Crisis document pack:** printed and offline copies of this Plan, business continuity plans, contact lists, templates and the stakeholder map, held by each CMT member.
- **Information management:** a single crisis workspace or folder ([location]) for sitreps, the decision log and approved messages, with restricted access.

12. First-hour actions

Use the activation checklist in Appendix A. In the first hour after activation, the CMT Chair makes sure that:

1. people are safe: emergency services called where needed; staff and visitors accounted for;
2. the CMT is convened, roles and deputies are confirmed, and the loggist has started the decision log;
3. the first situation briefing is given: what is known, what is not known, the impact on people, customers and critical operations, and the actions already taken;
4. the time of awareness is recorded and the regulatory clocks are identified (section 18), including CPS 230 para 41 (24 hours) and CPS 234 para 35 (72 hours);
5. the response teams are confirmed and are working under their plans (business continuity, cyber, data breach, DR);
6. immediate decisions are made to protect people, customers, data and critical operations, and recorded;
7. a holding statement is approved and ready (Appendix D), and staff are told what has happened and what to do;
8. the Board Chair is informed, or the time to do so is set; and

9. the next CMT meeting time and the sitrep rhythm are set.

13. First-day actions

Within the first [24 hours], the CMT should:

- agree **strategic objectives** for the response (for example: keep people safe; restore payments within tolerance; protect customer data; meet every regulatory obligation; maintain trust) and the priorities between them;
- confirm the status of each affected critical operation against its tolerance levels and decide whether to notify APRA under CPS 230 para 41;
- complete the first notification assessments for every obligation in section 18, recording decisions and reasons;
- approve the communications strategy and the first round of messages to staff, customers, regulators, service providers and, where needed, the media and the market;
- assess the welfare of affected staff and arrange support (section 19);
- set up a regular rhythm: sitreps every [2–4 hours], CMT meetings every [4–6 hours] in the acute phase;
- consider worst-case developments and prepare options in advance ("what if this gets worse?");
- arrange for fatigue management: rosters for CMT members and deputies, and handovers using the decision log and the latest sitrep;
- brief the Board, or the Board Chair and [Board Risk Committee] chair; and
- notify insurers as the policies require, through Legal.

14. Decision-making and logging

ISO 22361:2022 recognises that crisis teams must decide under uncertainty, time pressure and intense scrutiny. To support good decisions:

- **Use a simple structure** for each major decision: (1) What is the situation and what do we know? (2) What are our objectives and constraints? (3) What are the options and their consequences, including for customers and the vulnerable? (4) What do we decide, and why? (5) Who does what, by when? (6) When will we review it?
- **Challenge.** The Chair invites dissent and the Risk lead gives an independent view. Watch for common traps: waiting for perfect information, fixing on the first explanation, and group agreement without challenge.
- **Record every decision** in the decision log (Appendix C) at the time it is made: time,

decision, information relied on, options considered, reasons, owner and review time. The log is a key record for the Board, regulators, insurers, auditors, and any later inquiry or litigation.

- **Record decisions not to act** (for example not to notify, not to make a public statement) with the reasons, in the same way.
- **Legal privilege.** Where Legal directs, specific analysis may be prepared for the purpose of legal advice. The decision log itself should be written on the basis that it may be disclosed: factual, professional, no speculation or blame.
- **Keep the log in one place**, with backups, and retain it for at least **[7 years]**.

15. Situational awareness

The CMT needs a shared, current picture of the situation. The Crisis Management Coordinator makes sure that:

- a **situation report** is issued at an agreed rhythm, covering: what has happened; what is known and not known; impact on people, customers, critical operations (against tolerance), data, finances, regulators and reputation; actions under way; and decisions needed;
- information is drawn from the response teams, service providers, customer channels, complaints, social media and media monitoring, and external sources (for example emergency services, ASD, regulators or industry bodies);
- facts, assumptions and unconfirmed reports are clearly separated;
- a status board tracks each affected critical operation, the time the disruption started, the tolerance levels and the expected recovery time; and
- a timeline of key events is kept, to support notifications and the post-crisis review.

16. Stakeholder communications

Communications follow the business continuity communications strategy (CPS 230 para 39(e)) and the stakeholder map in Appendix E. Messages are clear, consistent, timely, honest and empathetic. Say what happened, what **[Organisation]** is doing, what the stakeholder should do, and when the next update will be.

Stakeholder	Channel	Prepared by	Approved by	Timing
-------------	---------	-------------	-------------	--------

Stakeholder	Channel	Prepared by	Approved by	Timing
Staff	Mass notification, intranet, manager briefings, phone	People lead / Communications lead	CMT Chair	First message within [2 hours] ; regular updates; before or at the same time as public statements
Customers and beneficiaries	Website banner, app, SMS, email, contact centre scripts, social media	Customer lead / Communications lead	CMT Chair, with Legal review	As soon as customers are, or may be, affected; regular updates
Board	Phone briefing, written sitrep	CMT Chair / Company Secretary	CMT Chair	Chair within [2 hours] ; full Board as agreed with the Chair
APRA	APRA's online notification form, then phone or email to the responsible supervisor	Legal and regulatory lead	[General Counsel / Head of Compliance] , with the CMT Chair informed	Within the deadlines in section 18; ongoing updates as agreed with APRA
ASIC, OAIC, AUSTRAC, ASD and other regulators or agencies	As each regulator requires	Legal and regulatory lead	[General Counsel / Head of Compliance]	Within the deadlines in section 18
Media	Statements, briefings, spokesperson	Communications lead	CMT Chair, with Legal review	Holding statement as soon as media interest is likely; never comment beyond the approved message

Stakeholder	Channel	Prepared by	Approved by	Timing
ASX and investors (listed entities)	ASX Market Announcements Platform	Company Secretary / Legal	[Board / Disclosure Committee] under the [Continuous Disclosure Policy]	Immediately, unless an exception in LR 3.1A applies; consider a trading halt
Material service providers and partners	Account managers, phone, email	Operations lead	Operations lead	As needed for the response and as contracts require
Insurers and brokers	As the policy requires	Finance lead / Legal	[General Counsel]	As the policy requires (often 'as soon as practicable')
Intermediaries, advisers, employers (super funds), industry bodies	Email, portal, phone	Customer lead	Communications lead	As needed

- **Only authorised spokespeople** speak for [Organisation]: [CEO], [Chair] and [named deputies]. All other staff refer enquiries to the Communications lead.
- **Market-sensitive information.** For listed entities, information that a reasonable person would expect to have a material effect on the price or value of [Organisation]'s securities must be disclosed to ASX immediately under Listing Rule 3.1, unless an exception in LR 3.1A applies. Do not release such information to the media before ASX.
- **Consistency.** Messages to regulators, customers, staff and the media must be consistent. Regulators should not learn of a material event from the media.
- **Accessibility.** Messages are in plain English, available in accessible formats and, where relevant, in languages other than English. Plan support for vulnerable customers and those in hardship.
- **Social media.** Monitor continuously; correct misinformation with facts; do not engage in argument.
- **Do not speculate** about cause, blame or the number of people affected until confirmed. Do not make promises that cannot be kept.

17. Customers and vulnerable customers

- Identify which customers are, or may be, affected, and which are vulnerable or in hardship.
- Decide what customers need to do, and what [Organisation] will do for them (for example fee waivers, hardship support, extensions, alternative ways to transact, priority claims handling).
- Increase contact centre and complaints capacity, and give staff scripts and authority to help.
- Tell customers about internal dispute resolution and AFCA where relevant.
- Where customers have suffered loss, plan customer remediation under the RiskFA Incident & Issues Management Standard (ASIC RG 277 where it applies).

18. Regulatory and external notifications

The Legal and regulatory lead keeps a notification tracker from activation, records the time of awareness for each obligation, and reports its status at every CMT meeting. The detailed obligations are in the RiskFA Incident & Issues Management Standard (section 10); the most time-critical in a crisis are:

Obligation	Applies to	When
Disruption to a critical operation outside tolerance (CPS 230 para 41): nature of the disruption, action taken, likely impact on business operations, timeframe for return to normal. The Board is also told, with a remediation plan (para 40).	APRA-regulated entities	APRA, as soon as possible and not later than 24 hours after suffering the disruption
Operational risk incident likely to have a material financial impact or a material impact on the ability to maintain critical operations (CPS 230 para 32). An incident notified under CPS 234 need not be notified again (footnote 11).	APRA-regulated entities	APRA, as soon as possible and not later than 72 hours after becoming aware

Obligation	Applies to	When
Information security incident that materially affected, or could have materially affected, the entity or customers, or that has been notified to another regulator in Australia or overseas (CPS 234 para 35)	APRA-regulated entities	APRA, as soon as possible and not later than 72 hours after becoming aware
Material information security control weakness the entity expects it cannot remediate in a timely manner (CPS 234 para 36)	APRA-regulated entities	APRA, not later than 10 business days after becoming aware
Suspected eligible data breach (Privacy Act Part IIIC, Notifiable Data Breaches scheme)	Entities covered by the Privacy Act	Assess within 30 calendar days ; if eligible, notify the OAIC and affected individuals as soon as practicable
Cyber security incident with a significant (s30BC) or relevant (s30BD) impact on a critical infrastructure asset (SOCI Act Part 2B)	Responsible entities for critical infrastructure assets	ASD within 12 hours (significant) or 72 hours (relevant) of becoming aware
Ransomware or cyber extortion payment (<i>Cyber Security Act 2024</i> s27)	Businesses with annual turnover above \$3 million , and SOCI Part 2B responsible entities	The designated Commonwealth body (Home Affairs and ASD, via the form on cyber.gov.au) within 72 hours of making the payment or becoming aware it was made
Reportable situation (Corporations Act s912DAA; NCCP Act s50B), including an investigation continuing for more than 60 days	AFS and credit licensees	ASIC within 30 calendar days of the reasonable-grounds trigger
Notifiable incident: death, serious injury or illness, or dangerous incident (<i>Work Health and Safety Act 2011</i> (Cth) ss 35, 38, and state and territory equivalents)	Persons conducting a business or undertaking	The WHS regulator immediately after becoming aware
Price-sensitive information (ASX Listing Rule 3.1)	Listed entities	ASX immediately , unless an exception in LR 3.1A applies

Obligation	Applies to	When
Insurance, contractual and overseas regulator notifications	All	As the policy, contract or law requires

APRA notifications are made electronically using the form on APRA's website (CPG 230 para 14). A notification should not wait for full information: give what is known, say what is not yet known, and update APRA as the situation develops. Delete obligations that do not apply to you and confirm current requirements with the regulator's guidance or your legal adviser.

19. Staff safety and welfare

[Organisation] has a primary duty of care to ensure, so far as is reasonably practicable, the health and safety of workers and others affected by its work (*Work Health and Safety Act 2011* (Cth) s19, and state and territory equivalents). In a crisis, the People lead makes sure that:

- all staff, contractors and visitors at affected sites are accounted for, and the families of anyone injured are contacted appropriately and with care;
- staff are told what has happened, what to do, where to work and whom to contact, before they hear it from the media where possible;
- the employee assistance program and, where needed, trauma or critical incident support are offered promptly and repeated over the following weeks;
- workloads, rosters and breaks are managed for response teams and the CMT, including fatigue limits for extended crises;
- psychosocial hazards (for example abusive customers, distressing content, prolonged pressure) are managed;
- staff who are personally affected (for example by a natural disaster) have flexible leave and support; and
- notifiable WHS incidents are reported to the regulator immediately and the incident site is preserved where the law requires.

20. Coordination with business continuity and cyber incident response

- **Business continuity.** The Operations lead brings the status of every affected critical operation against its tolerance levels to each CMT meeting. The CMT decides priorities between critical operations when resources conflict, approves major contingency arrangements, and confirms the CPS 230 para 41 notification decision. Business continuity teams run the recovery under their plans (RiskFA Business Continuity Policy).
- **Cyber incident response.** The Technology and security lead links the CMT with the Cyber Incident Response Team. The CMT decides strategic matters (for example taking critical services offline for long periods, public statements and Board engagement), and decisions reserved to the Board under the RiskFA Cyber Incident Response Plan go to the Board. The CMT uses out-of-band channels whenever an attacker may have access to [Organisation]'s systems.
- **Data breach response.** The data breach response team runs the assessment and notification process under the RiskFA Data Breach Response Plan and reports to the CMT.
- **Service providers.** Where the crisis starts at a material service provider, the Operations lead keeps a direct line to the provider's crisis team and asks for regular updates, evidence and recovery times.
- **Recovery and exit planning.** Where a crisis threatens financial soundness, the Finance lead brings the [Recovery and Exit Plan] or [Liquidity Contingency Plan] to the CMT, and the Board is engaged early.

21. Board engagement

- The CMT Chair informs the Board Chair within [2 hours] of activation and agrees how and how often the Board will be briefed.
- The Board oversees; the CMT manages. The Board makes the decisions reserved to it and holds management to account, but does not run the response.
- The Board is told of any failure to meet a tolerance level, with a remediation plan (CPS 230 para 40), and of every regulatory notification.
- Board members are reminded not to comment publicly and to refer enquiries to the Communications lead.
- [Board members] take part in at least one crisis exercise each [year] (section 24).

22. Stand-down and recovery

The CMT Chair decides when to stand down the CMT, on the CMT's advice. Before stand-down, the CMT confirms that:

- people are safe and welfare support is in place for as long as it is needed;
- critical operations are back within tolerance or are on a stable, managed path to recovery under the business continuity plans;
- the immediate threat is contained, and no further strategic decisions are expected;
- all regulatory notifications are made, and follow-up obligations (for example updates to APRA) are assigned;
- a stand-down message is sent to staff and, where appropriate, customers and other stakeholders;
- remaining actions are handed over to named owners and recorded under the RiskFA Incident & Issues Management Standard, including customer remediation;
- the decision log, sitreps and records are complete and secured; and
- the post-crisis review is scheduled.

The stand-down decision and time are recorded. The CMT can be re-activated at any time if the situation worsens.

23. Post-crisis review

A post-crisis review is completed within [30 business days] of stand-down for every CMT activation, led by [the CRO or an independent person not involved in the response]. It uses the post-incident review requirements of the RiskFA Incident & Issues Management Standard and covers:

- the timeline, from the first sign of the event to stand-down, drawn from the decision log and sitreps;
- the impact on people, customers, critical operations (against tolerance), finances, regulators and reputation;
- how well the response worked: activation speed, CMT roles and deputies, decision-making, situational awareness, communications, coordination with response teams and service providers, and welfare support;
- whether every regulatory notification was made on time;
- the root causes of the event and of any weaknesses in the response, and the extent of condition; and

- actions, owners and due dates, including changes to this Plan, business continuity plans, controls and training.

The review is reported to the executive and the [Board Risk Committee] . Lessons are shared with response teams and used to design the next exercise.

24. Training and exercises

ISO 22361:2022 treats training, validation and learning from crises as part of building a crisis management capability. CPG 230 para 37 notes that testing the business continuity plan should build experience in managing a crisis. [Organisation] runs:

Activity	Participants	Minimum frequency
Induction briefing on this Plan and the member's role	New CMT members and deputies	Before taking on the role
CMT tabletop exercise on a severe but plausible scenario (for example ransomware with data theft; loss of a material service provider; natural disaster affecting staff and sites)	CMT members and deputies; response team leads	At least [annually] , usually as part of the annual business continuity exercise required by CPS 230 para 42
Notification and call tree test (including the out-of-band bridge)	CMT and deputies	At least [twice a year]
Spokesperson and media training	Authorised spokespeople	Every [2 years]
Board crisis exercise or briefing	[Board members]	At least [annually]
Loggist training	Loggists and deputies	Before taking on the role, refreshed [annually]
Joint exercise with a material service provider	CMT or operations lead with the provider	Within the business continuity testing cycle (CPS 230 para 43)

- Exercises should test decision-making under pressure, not just the plan, and should include injects such as media enquiries, regulator calls and worsening facts.

- Exercise reports use the RiskFA Business Continuity Policy test and exercise report template, and issues are tracked under the RiskFA Incident & Issues Management Standard.
- Where scenarios overlap, exercises are combined with business continuity, cyber incident response (CPS 234 para 26) and recovery plan testing.

25. Plan maintenance

- The [Crisis Management Coordinator] checks CMT membership, deputies and contact details at least [quarterly], and after any change in executive roles.
- The Plan is reviewed at least [annually] and after every activation and the annual exercise.
- Printed and offline copies are replaced whenever the Plan changes, and old copies are destroyed.
- Templates, holding statements and the stakeholder map are reviewed at least [annually].

26. Related documents

- The RiskFA Business Continuity Policy, Incident & Issues Management Standard, Cyber Incident Response Plan, Data Breach Response Plan and Risk Management Framework
- [Business Continuity Plans], [Disaster Recovery Plans], [Emergency Response Procedures], [Recovery and Exit Plan], [Liquidity Contingency Plan]
- [Media and Communications Policy], [Continuous Disclosure Policy], [Work Health and Safety Policy]
- APRA: CPS 230 *Operational Risk Management* (2026) and CPG 230 (July 2026); CPS 234 *Information Security*
- ASIC: RG 78 *Breach reporting by AFS licensees and credit licensees*; RG 277 *Consumer remediation*; OAIC: Notifiable Data Breaches guidance; ASX Listing Rules Chapter 3 and Guidance Note 8
- Standards: ISO 22361:2022 *Security and resilience — Crisis management — Guidelines*; ISO 22301:2019 *Business continuity management systems — Requirements*

Appendix A. Activation checklist

#	Action	Who	Done (time)
1	People safe? Emergency services called if needed; staff and visitors accounted for	People lead / site lead	☐
2	Activation criteria met (section 8) recorded; activation decision and time recorded	Activation authority	☐
3	CMT and deputies notified; meeting time and channel set (out-of-band if systems may be compromised)	Crisis Management Coordinator	☐
4	Loggist appointed; decision log opened	Crisis Management Coordinator	☐
5	Time of awareness recorded for each regulatory clock; notification tracker opened	Legal and regulatory lead	☐
6	Affected critical operations listed with disruption start time and tolerance levels	Operations lead	☐
7	Response teams activated under their plans (BCP, cyber, data breach, DR)	Operations lead / Technology and security lead	☐
8	First situation briefing given	Incident Executive / Operations lead	☐
9	Holding statement approved and ready; first staff message sent	Communications lead / CMT Chair	☐
10	Board Chair informed	CMT Chair	☐
11	Insurers and key service providers considered for notification	Legal / Operations lead	☐
12	Next meeting time and sitrep rhythm set	Crisis Management Coordinator	☐

Appendix B. CMT meeting agenda template

#	Item	Lead	Time
1	Roll call, roles and deputies confirmed; loggist ready	Crisis Management Coordinator	[2 min]
2	People: safety and welfare	People lead	[3 min]
3	Situation update: what has changed since the last meeting; what is known and not known	Incident Executive / Operations lead	[5 min]
4	Critical operations against tolerance; recovery progress and expected times	Operations lead	[5 min]
5	Customers: impact, vulnerable customers, contact centre and complaints	Customer lead	[3 min]
6	Regulatory notifications: tracker status, deadlines due, regulator contact	Legal and regulatory lead	[3 min]
7	Communications: media and social media, messages for approval	Communications lead	[5 min]
8	Financial, liquidity and market matters	Finance lead	[3 min]
9	Decisions needed: options, recommendation, decision, owner (recorded in the decision log)	CMT Chair	[10 min]
10	Review of earlier decisions still in force	CMT Chair	[3 min]
11	Worst-case outlook: what could get worse and how we would respond	Risk lead	[3 min]
12	Actions, owners and next meeting time; Board update due?	Crisis Management Coordinator	[2 min]

Appendix C. Decision log template

Ref	Date / time	Decision (or decision not to act)	Information relied on	Options considered	Reasons	Owner	Review time
[D-01]	[]	[]	[]	[]	[]	[]	[]
[D-02]	[]	[]	[]	[]	[]	[]	[]
[D-03]	[]	[]	[]	[]	[]	[]	[]

Write entries at the time, in plain factual language. Never delete or overwrite an entry: if a decision changes, add a new entry that refers to the earlier one. The log is signed off by the CMT Chair at stand-down.

Appendix D. Holding statement template

Use within the first [1–2 hours] when the facts are still unclear. Approved by the CMT Chair, with Legal review. Adapt for each audience and channel.

Part	Template wording
What we know	" [Organisation] is aware of [a brief, factual description, for example 'a disruption to our online banking and app services' or 'a cyber security incident affecting some of our systems'] that began at [time] on [date]."
What we are doing	"We are working urgently to [restore services / investigate and contain the incident], and we have [activated our business continuity arrangements / engaged specialist support]. We have informed the relevant authorities."
What it means for you	"Customers can still [use ATMs, branches or phone banking on number]. At this stage we have no evidence that [customers' money / personal information] has been affected." (Use the second sentence only if confirmed.)
Our people and customers	"The safety of our [customers and staff] is our priority." / "We apologise for the inconvenience and concern this is causing."
Next update	"We will provide a further update by [time], at [website / channel]."
Contact	Media: [name, phone, email]. Customers: [contact centre number], [website].

Do not speculate about the cause, blame anyone, give numbers that are not confirmed, or promise timeframes that cannot be guaranteed. For listed entities, check with the Company Secretary whether the information must first go to ASX under Listing Rule 3.1.

Appendix E. Stakeholder map

Stakeholder group	Main concerns in a crisis	Owner on the CMT	Primary channel	Contact details held in
Staff and contractors	Safety, what to do, job security, welfare	People lead	Mass notification, managers, intranet	[HR system / notification tool]
Customers and beneficiaries (incl. vulnerable customers)	Access to money, cover or service; data safety; what to do	Customer lead	Website, app, SMS, email, contact centre	[CRM]
Board	Oversight, decisions reserved to the Board, regulatory and legal exposure	CMT Chair	Phone, sitrep	[Company Secretary list]
APRA	Critical operations against tolerance, customer impact, prudential soundness, notification	Legal and regulatory lead	APRA online form; responsible supervisor	[Regulator contact list]
ASIC, OAIC, AUSTRAC, ASD and other agencies	Consumer harm, breaches, data, cyber, financial crime	Legal and regulatory lead	As each regulator requires	[Regulator contact list]
Media	What happened, impact, accountability	Communications lead	Statements, spokesperson	[Media list]
ASX, shareholders and investors (listed entities)	Price-sensitive information, financial impact	Finance lead / Company Secretary	ASX announcements, investor relations	[IR list]
Material service providers	Their role in the event and recovery; contract obligations	Operations lead	Account managers, crisis contacts	[Service provider register]

Stakeholder group	Main concerns in a crisis	Owner on the CMT	Primary channel	Contact details held in
Insurers and brokers	Notification, cover, claims	Finance lead / Legal	As the policy requires	[Insurance register]
Intermediaries, advisers, employers and partners	Impact on their clients and operations	Customer lead	Portal, email, phone	[Partner list]
Emergency services, government and industry bodies	Public safety, system-wide impact, coordination	CMT Chair / Operations lead	Phone, liaison officers	[Emergency contact list]



[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.](#)