

Cyber Incident Response Plan

How to prepare for, detect, contain, eradicate, recover from and learn from cyber security incidents, with playbooks, decision rights, notification deadlines and ready-to-use templates. 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 and contact numbers, set the timeframes to match your size and risk appetite, delete obligations and playbooks that do not apply to you, and approve the Plan through your governance process. Keep a printed or offline copy: during a serious cyber incident your 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	Cyber Incident Response Plan (Information Security Incident Response Plan)
Organisation	[Organisation name]
Document owner	[Chief Information Security Officer]
Approved by	[Board Risk Committee]
Version / date approved	[1.0] / [date]
Review cycle	Reviewed and tested at least [annually] (CPS 234 para 26), and after any Critical or High cyber incident, a material change to systems, service providers or regulation, or a significant exercise finding
Parent documents	the RiskFA Cyber Security Policy; the RiskFA Incident & Issues Management Standard
Offline copies held by	[CISO, CTO, CRO, General Counsel, Head of Communications, Incident Manager on-call]

1. Purpose

This Plan sets out how [Organisation] prepares for, detects, analyses, contains, eradicates, recovers from and learns from **cyber security incidents**. It ensures that:

- cyber incidents are recognised quickly and handled by a trained team with clear roles and decision rights;
- harm to customers, critical operations, information assets and the organisation is limited;
- evidence is preserved so that the cause can be found and legal options kept open;
- the Board, regulators, law enforcement, customers and other parties are told what they need to know, within the required timeframes; and
- lessons are learned and the root cause is fixed, so that the incident does not recur.

This Plan is [Organisation]'s **information security response plan** for the purposes of APRA Prudential Standard CPS 234 *Information Security* paras 24 to 26, where CPS 234 applies. It is aligned to NIST SP 800-61 Rev. 3 and the ISO/IEC 27035 series (section 6).

2. Scope

This Plan applies to:

- all employees, contractors, directors and officers of [Organisation] and its subsidiaries;
- all information assets (information and information technology, including software, hardware, data, cloud services and operational technology) owned or used by [Organisation], wherever they are located; and
- cyber incidents at material service providers and other third parties that affect [Organisation]'s information assets, services, data or customers.

It covers incidents that affect the confidentiality, integrity or availability of information assets, including malware and ransomware, cyber extortion, unauthorised access, data theft, business email compromise, denial of service, insider misuse, and compromise of customer accounts or of a service provider.

Physical incidents, natural hazards and non-cyber technology outages are handled under the RiskFA Business Continuity Policy and the RiskFA Crisis Management Plan, and privacy incidents that do not involve a cyber cause under the RiskFA Data Breach Response Plan. Where an incident has both a cyber and a non-cyber element, this Plan applies to the cyber element.

3. Relationship to other documents

Document	How it works with this Plan
The RiskFA Incident & Issues Management Standard	Every cyber incident is recorded in the incident register, rated Critical, High, Medium or Low , escalated and closed under that Standard. This Plan adds the cyber-specific response. Root cause, extent of condition, issues, actions and customer remediation follow the Standard.
the RiskFA Cyber Security Policy	Sets the security objectives, roles and controls. This Plan is the response part of that policy.
The RiskFA Data Breach Response Plan	Applies whenever personal information may have been accessed, disclosed or lost. It runs alongside this Plan and owns the Notifiable Data Breaches (NDB) assessment and notification (section 19 and Appendix C).
the RiskFA Business Continuity Policy	Invoked when a cyber incident disrupts, or is likely to disrupt, a critical operation or other important service. Business continuity keeps services running while this Plan deals with the threat.
the RiskFA Crisis Management Plan	Invoked for Critical incidents. The Crisis Management Team takes strategic decisions (section 7); the Cyber Incident Response Team runs the technical response.
[Third Party / Material Service Provider Management Policy]	Sets the notification and cooperation terms that service providers must meet (section 21).

4. Key definitions

Term	Meaning
Cyber security event	An observed occurrence in a system or network that may indicate a security problem, such as an alert, an unusual login or a failed attack. Most events are not incidents.
Cyber security incident	One or more events that have, or could have, an adverse effect on the confidentiality, integrity or availability of an information asset. For APRA-regulated entities this is an information security incident under CPS 234.
Material information security incident	An information security incident that materially affected, or had the potential to materially affect, financially or non-financially, [Organisation] or the interests of depositors, policyholders, beneficiaries or other customers (CPS 234 para 35(a)).
Indicator of compromise (IOC)	Technical evidence of an intrusion, such as a malicious file hash, IP address, domain or account.
Cyber Incident Response Team (CIRT)	The team that runs the operational response (section 7).
Containment	Actions that stop an incident from spreading or causing more harm, such as isolating devices, disabling accounts or blocking traffic.
Eradication	Removing the attacker, malware and the means of access from the environment.
Recovery	Restoring systems and services to normal operation from trusted sources, with monitoring for re-infection.
Ransomware payment	A payment or benefit given to an entity that has made a demand in connection with a cyber security incident, where the payment is directly related to the demand (<i>Cyber Security Act 2024</i> s26).
Eligible data breach	Unauthorised access to, unauthorised disclosure of, or loss of personal information that is likely to result in serious harm to any of the individuals concerned, and where remedial action has not prevented that likely harm (<i>Privacy Act 1988</i> ss 26WE, 26WF).
Chain of custody	A documented, unbroken record of who collected, held, transferred and examined each item of evidence, and when.

Term	Meaning
Incident, Near miss, Issue, Breach, Root cause, Extent of condition, Critical operation, Material service provider, Reportable situation	As defined in the RiskFA Incident & Issues Management Standard.

5. Principles

1. **Report early.** Anyone who suspects a cyber incident reports it straight away to the [Security Operations Centre / IT Service Desk] on [phone number]. A false alarm costs little; a late report can cost a great deal.
2. **Safety and customers first.** Protect people, customers and critical operations before systems and convenience.
3. **Contain fast, but think first.** Act quickly to stop harm, but do not destroy evidence or alert the attacker without need. Isolate rather than wipe or switch off.
4. **Assume the attacker can see you.** Use out-of-band communications for the response if email, chat or the network may be compromised.
5. **Write it down.** Record every action and every decision with the time, the person and the reason (Appendices J and K).
6. **Meet the clock.** Regulatory deadlines run from when [Organisation] becomes aware, not from when the investigation finishes. Some are as short as 12 hours.
7. **One rating language.** Cyber severity always maps to the common rating (Critical, High, Medium, Low) so that everyone, up to the Board, understands it.
8. **Recover clean.** Restore from known-good sources and verify before returning systems to service.
9. **Learn and fix the cause.** Every Critical and High incident has a post-incident review and its root cause is fixed.

6. Standards and response phases

This Plan follows recognised standards, so that internal teams, service providers, external responders and regulators share the same terms:

- **NIST SP 800-61 Rev. 3** *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile* (April 2025). It

- supersedes Rev. 2 (2012) and places incident response within the six Functions of the NIST Cybersecurity Framework 2.0: **Govern, Identify and Protect** (preparation and improvement), and **Detect, Respond and Recover** (incident response itself).
- **ISO/IEC 27035** *Information security incident management*: Part 1:2023 (principles and process: plan and prepare; detection and reporting; assessment and decision; responses; lessons learnt), Part 2:2023 (plan and prepare for incident response), Part 3 (ICT incident response operations) and Part 4:2024 (coordination across organisations).
 - **ASD's Australian Cyber Security Centre** guidance, including the Ransomware Playbook and incident reporting guidance on cyber.gov.au.

[Organisation] uses six practical phases. They map to the standards as follows:

Phase in this Plan	NIST CSF 2.0 Function (SP 800-61r3)	ISO/IEC 27035-1 phase	Section
1. Prepare	Govern, Identify, Protect	Plan and prepare	11
2. Detect and analyse	Detect; Respond (incident analysis, triage)	Detection and reporting; Assessment and decision	12
3. Contain	Respond (incident mitigation)	Responses	13
4. Eradicate	Respond (incident mitigation)	Responses	14
5. Recover	Recover	Responses	14
6. Post-incident review	Identify (improvement)	Lessons learnt	15

The phases overlap in practice. Containment, analysis and notification often run at the same time, and new findings can send the team back to an earlier phase.

7. Incident response team and governance

The response is organised in three tiers. For Medium and Low incidents only the CIRT is usually needed. High incidents bring in the Incident Executive. Critical incidents also activate the Crisis Management Team under the RiskFA Crisis Management Plan.

Tier	Who	Purpose
------	-----	---------

Tier	Who	Purpose
Crisis Management Team (strategic)	[CEO] (chair), [CRO], [General Counsel], [CISO], [CTO], [Chief Operating Officer], [Head of Communications], [Chief Customer Officer]	Strategic decisions: taking critical services offline for long periods, ransom and extortion decisions, public statements, Board and regulator engagement.
Incident Executive (tactical)	[CISO] (or [CTO] if the CISO is unavailable)	Owns the response, sets priorities, approves major containment, keeps executives and Compliance informed.
Cyber Incident Response Team (operational)	Incident Manager, security analysts, IT operations, cloud and network engineers, application owners, external responders	Investigates, contains, eradicates, recovers, preserves evidence and keeps the incident log.

7.1 Roles

Role	Primary / deputy	Responsibilities
Incident Executive	[CISO] / [CTO]	Accountable for the response; declares the incident severity; approves containment with business impact; escalates to the Crisis Management Team; the incident owner under the RiskFA Incident & Issues Management Standard for Critical and High cyber incidents.
Incident Manager	[Head of Security Operations] / [Security Operations Lead]	Runs the CIRT day to day; coordinates tasks and shifts; keeps the incident log and decision log; chairs regular status calls; manages handovers.
Technical Lead	[Lead Security Engineer] / [External IR provider lead]	Leads analysis, scoping, containment and eradication; directs forensic work.
IT Operations / Recovery Lead	[Head of Infrastructure] / [Cloud Platform Lead]	Carries out isolation, restores from backup, rebuilds systems and confirms they are clean.
Business Impact Lead	[Chief Operating Officer] / [Head of Business Continuity]	Assesses impact on customers and critical operations against tolerance levels; invokes business continuity.
Legal Lead	[General Counsel] / [Senior Legal Counsel]	Legal privilege, engagement of external lawyers and forensic firms, law enforcement, contracts, insurance, extortion and sanctions questions.
Compliance and Regulatory Lead	[Head of Compliance] / [Regulatory Affairs Manager]	Assesses and makes all regulatory notifications (section 19); keeps the regulator notification checklist (Appendix L).
Privacy Lead	[Privacy Officer] / [Deputy Privacy Officer]	Runs the RiskFA Data Breach Response Plan and the NDB assessment when personal information may be affected.
Risk Lead	[CRO] / [Head of Operational Risk]	Confirms the rating, second line challenge, Board Risk Committee escalation, link to the incident register.

Role	Primary / deputy	Responsibilities
Communications Lead	[Head of Communications] / [Media Manager]	Drafts and coordinates internal, customer and media communications for approval (section 18).
Customer Lead	[Chief Customer Officer] / [Head of Contact Centre]	Customer contact, scripts, vulnerable customers, complaints and remediation.
Third Party Lead	[Head of Procurement / Vendor Management]	Engages affected service providers and enforces contractual notification and cooperation terms.
Human Resources Lead	[Head of People]	Insider threat matters, staff welfare and staff communications.
Scribe	[Nominated analyst or PMO]	Keeps the incident and decision logs in real time.

Each role must have a named deputy. Contact details for all roles, including personal mobile numbers, are held in the contact list (Appendix I) and in the offline copies of this Plan.

7.2 Decision rights

The following people may make these decisions without waiting for further approval. Each decision is recorded in the decision log (Appendix K) with the reason.

Decision	Who may decide	Notes
Isolate an endpoint, server or user account; block an IP address, domain or email sender; reset credentials	Any security analyst or the Incident Manager	Do not wait for approval when there is active spread or data theft. Inform the system owner as soon as practicable.
Isolate a network segment, cloud tenant or business application; disable remote access or a service provider connection	Incident Manager, with Incident Executive approval (retrospective approval within [1 hour] if urgent)	Consider the impact on critical operations; tell the Business Impact Lead.

Decision	Who may decide	Notes
Take a customer-facing service or critical operation offline	Incident Executive for up to [4 hours] ; [CEO] (or Crisis Management Team) beyond that or for multiple critical operations	Immediate action is allowed to protect customers or data. Business continuity is invoked and the CPS 230 tolerance clock is tracked.
Disconnect [Organisation] from the internet or from payment and settlement systems	[CEO] on the advice of the Incident Executive	Tell [payment scheme / settlement system operators] as their rules require.
Declare or change the incident severity	Incident Executive; Risk Lead confirms the common rating	Lowering a Critical rating needs CRO approval (RiskFA Incident & Issues Management Standard).
Engage the external incident response or forensics provider under retainer	Incident Executive, with engagement through the Legal Lead	Engage through [General Counsel / external law firm] where privilege may be claimed (section 17).
Engage other external lawyers, crisis communications or negotiation support	Legal Lead / [CEO]	Within the delegated spend of [\$X] .
Spend on the response beyond normal delegations	Incident Executive up to [\$X] ; [CEO] above	Recorded for insurance and loss reporting.
Notify regulators	Compliance and Regulatory Lead, with Legal Lead review	Must not be delayed for approvals beyond the deadline. CEO informed before or as soon as possible after lodgement.
Report to police or engage ASD	Incident Executive or Legal Lead	Early engagement with ASD is encouraged (section 20).
Public or customer statements	[CEO] , on the advice of the Communications and Legal Leads	Holding statements pre-approved in Appendix A may be used by the Communications Lead.

Decision	Who may decide	Notes
Any engagement with an extortionist, or any ransom or extortion payment	Board (or [Board Chair and CEO] where the Board cannot be convened in time), on the advice of the Crisis Management Team and external legal advice	See Appendix A. No one else may communicate with or pay an extortionist.

8. Severity classification

The Incident Executive declares a cyber severity as soon as an incident is confirmed, using the realistic worst case. Cyber severity is the same as the common rating in the RiskFA Incident & Issues Management Standard, so a Critical cyber incident is a Critical incident for all purposes. If unsure, choose the higher severity. Re-assess at every status update and record the reason for any change.

Rating	Typical cyber indicators (any one is enough)	Response
Critical	Material information security incident (CPS 234 para 35(a)); critical operation disrupted or likely to be disrupted beyond tolerance; ransomware encryption of production or backup systems; confirmed theft of large volumes of customer or sensitive data, or a likely large-scale eligible data breach; attacker control of privileged identity (for example domain or cloud administrator); extortion demand; likely national media attention; significant impact on a SOCI critical infrastructure asset	CIRT, Incident Executive and Crisis Management Team activated immediately. Escalation within [1 hour] to CEO, CRO, General Counsel and accountable persons; Board Risk Committee chair within [24 hours]. Notification assessment started immediately.
High	Confirmed compromise of a sensitive system or privileged account, contained to a limited area; data exfiltration of limited scope, or a likely eligible data breach; disruption to a critical operation within tolerance; successful business email compromise with payment loss above [\$100k]; sustained denial of service affecting customers; compromise of a material service provider affecting [Organisation]'s data or services	CIRT and Incident Executive activated. Escalation to CRO and Head of Compliance within [4 hours] and in any case within [24 hours]. APRA materiality decision within [24 hours].

Rating	Typical cyber indicators (any one is enough)	Response
Medium	Malware or unauthorised access contained to a small number of non-critical systems or accounts; customer account takeover affecting a small number of customers; denial of service with limited customer impact; phishing with credentials compromised but no evidence of misuse	CIRT handles. Incident Executive informed within [1 business day]. Second line informed within [2 business days].
Low	Attempted attack blocked; a single infected device cleaned with no data exposed; policy breach with no data exposed	Handled by the security operations team; recorded in the register.

Severity sets the internal response. It does **not** decide whether a matter must be notified. Every cyber incident that may involve personal information, a critical operation, a critical infrastructure asset, a ransomware payment or another regulator is sent to the Compliance and Regulatory Lead, whatever its severity.

9. Activation and escalation

1. Anyone who suspects a cyber incident reports it to [Security Operations Centre / IT Service Desk] on [phone] or [email / portal]. Out of hours, call the on-call Incident Manager on [phone].
2. The security operations team triages the report within [30 minutes] (Critical or High indicators) or [4 hours] (others).
3. If an incident is confirmed or likely, the Incident Manager opens an incident record, starts the incident log and calls the Incident Executive.
4. The Incident Executive declares the severity and activates the response tier (section 7).
5. The Risk Lead records the incident in the incident register the same day for Critical and High incidents, as the RiskFA Incident & Issues Management Standard requires.
6. The Compliance and Regulatory Lead and, where personal information may be involved, the Privacy Lead are brought in for every Critical and High incident, and for any incident that may trigger a notification.
7. Status calls are held every [2 hours] (Critical) or [twice daily] (High) until the incident is contained.

Use the first-hour checklist (Appendix H) for every Critical and High incident.

10. Out-of-band communications

Attackers who control a network often read email and chat. For Critical and High incidents, and whenever identity systems or email may be compromised:

- move response communications to the pre-arranged out-of-band channel: [separate messaging tenancy / secure messaging app / bridge line number] ;
- do not discuss the incident in the corporate email, chat or ticketing system until the Technical Lead confirms they are safe;
- keep a printed or offline copy of this Plan, the contact list and key system diagrams; and
- verify the identity of anyone who joins the response by a call-back to a known number.

11. Phase 1: Prepare

Preparation is what makes the response work. [Organisation] maintains:

- this Plan, the playbooks in Appendices A to G, and up-to-date contact lists, including after-hours numbers for key people and service providers;
- an inventory of information assets, their owners and their criticality, linked to critical operations and their tolerance levels;
- logging and monitoring to detect incidents in a timely manner (CPS 234 para 23), with log retention of at least [12 months] for security-relevant logs [and longer where law requires] ;
- a retainer with an external incident response and forensics provider [name], and pre-agreed engagement terms through [external law firm] ;
- cyber insurance, with the insurer's notification requirements and approved provider panel recorded in Appendix I;
- backups of critical systems that are protected from tampering (for example offline or immutable), with restoration tested at least [annually] for critical systems;
- privileged access controls, multi-factor authentication and the ability to reset all privileged credentials quickly;
- pre-approved holding statements and customer scripts (Appendix A);
- out-of-band communications (section 10);
- contractual notification, cooperation and evidence-access terms with material service providers (section 21); and
- training for CIRT members and exercises at least [annually] (section 22).

Preparation draws on ASD's *Essential Eight* mitigation strategies and the *Information Security*

Manual as good practice, and on the NIST CSF 2.0 Govern, Identify and Protect Functions.

12. Phase 2: Detect and analyse

The aim is to confirm whether an incident is occurring, understand its scope and severity, and make early decisions on containment and notification.

- **Sources of detection:** security monitoring alerts, staff and customer reports, service provider notices, ASD or law enforcement advice, threat intelligence, extortion messages, and media or dark web reports.
- **Triage:** confirm the facts; identify affected systems, accounts, data and customers; record the time **[Organisation]** **became aware**, because notification clocks run from it.
- **Scope:** establish how the attacker got in, what they accessed, whether data left the network, whether they still have access, and whether other systems or entities are affected (extent of condition).
- **Data impact:** if personal information may have been accessed, disclosed or lost, start the RiskFA Data Breach Response Plan and the 30-day NDB assessment immediately.
- **Severity:** declare and record the severity (section 8).
- **Notification triage:** within **[4 hours]** of a Critical or High incident being declared, the Compliance and Regulatory Lead completes a first pass of Appendix L and records which clocks may be running.

Analysis must preserve evidence (section 16). Do not run untested tools on affected systems, and do not let anyone without forensic training 'look around' on a compromised machine.

13. Phase 3: Contain

Containment stops the incident from spreading and buys time. The Technical Lead proposes a containment strategy and the Incident Executive approves it, taking account of:

- the harm that continued attacker access could cause, compared with the business impact of containment;
- the need to preserve evidence (capture memory and logs before isolating where it is safe to do so);
- the risk that visible containment tips off the attacker and prompts destructive action, such as early encryption or data release; and
- the impact on critical operations and customers, and the business continuity options.

Short-term containment

Longer-term containment

Short-term containment	Longer-term containment
Network-isolate affected devices (do not switch off unless instructed)	Rebuild or replace affected systems in a clean environment
Disable or reset compromised accounts, revoke sessions and tokens	Reset all privileged credentials, service accounts and keys where the identity system may be compromised
Block malicious IP addresses, domains, files and email senders	Tighten segmentation and access rules
Suspend affected service provider connections and remote access	Apply patches and configuration changes for the exploited weakness
Protect backups by disconnecting or locking them	Increase monitoring for the IOCs and attacker techniques found

14. Phases 4 and 5: Eradicate and recover

14.1 Eradicate

- Remove malware, persistence mechanisms, attacker accounts and unauthorised changes.
- Close the access route (for example the vulnerability, stolen credential or service provider connection).
- Confirm eradication across the whole environment, not only the systems first found. Assume the attacker had more access than first seen until proven otherwise.
- Do not start eradication until the scope is understood. Premature eradication often leaves the attacker inside.

14.2 Recover

- Restore in priority order: identity and security systems first, then critical operations in order of their tolerance levels, then other services.
- Restore from backups or images that have been checked as clean and taken before the earliest sign of compromise.
- Test restored systems and confirm they are clean before reconnecting them; apply heightened monitoring for at least [30 days].
- The business owner and the Technical Lead jointly approve the return to service.
- Track recovery against CPS 230 tolerance levels for each affected critical operation and keep the Board and APRA informed as required (section 19).

The Incident Executive declares the incident **contained** and then **resolved**. The incident is closed under the RiskFA Incident & Issues Management Standard once notifications, customer remediation and issues are in place.

15. Phase 6: Post-incident review

- A post-incident review is held for every Critical and High cyber incident within [20 business days] of resolution, and for others at the CISO's discretion.
- The review is blameless in tone but honest about failures. It covers the timeline, root cause, extent of condition, how well this Plan and the playbooks worked, what was missed, and what will change (Appendix M).
- Every control gap found is raised as an issue with an owner and due date under the RiskFA Incident & Issues Management Standard.
- Material control weaknesses that cannot be remediated in a timely manner are notified to APRA within 10 business days (CPS 234 para 36) and escalated to the Board or senior management.
- The review is reported to the executive and the Board Risk Committee, and lessons are used to update this Plan, playbooks, training and the risk and control assessment.

16. Evidence preservation and chain of custody

Evidence supports the investigation, insurance claims, regulator inquiries and any legal action. From the moment an incident is suspected:

- **Do not** wipe, re-image, power off or reboot affected systems, delete emails or messages, or contact the attacker, unless the Technical Lead approves.
- Capture volatile evidence first where safe (memory, running processes, network

connections), then disk images, logs (endpoint, server, network, identity, cloud and email), and copies of extortion messages, ransom notes and attacker communications.

- Extend log retention and suspend automated deletion for affected systems and mailboxes.
- Use write-blocking and hashing (for example SHA-256) for forensic images, and work on copies, not originals.
- Record chain of custody for each item: description, source, date and time collected, collector, hash value, storage location, and every transfer and access (Appendix J includes the fields).
- Store evidence securely with access limited to named people. Keep it for at least [7 years] or as Legal directs.
- Agree evidence handling with any external forensic provider, law enforcement and the insurer at engagement.

17. Legal professional privilege

Legal professional privilege may protect some communications and documents created for the dominant purpose of giving legal advice or for actual or anticipated litigation. It can help protect sensitive investigation findings, but it is never certain and must not delay the response or a required notification.

- The Legal Lead decides at the start whether to seek privilege, and if so the external forensic provider is engaged by, and reports to, [General Counsel / external law firm].
- Documents prepared for operational purposes (for example remediation, Board updates or regulator reporting) may not be privileged even if prepared by lawyers. Keep operational records and legal advice separate, and follow Legal's instructions on marking and distribution.
- Facts are not privileged. Regulators may still require them using their own powers.
- Information given in a ransomware payment report, or voluntarily to the National Cyber Security Coordinator, does not, by that fact alone, affect a claim of privilege (*Cyber Security Act 2024* ss 31, 41).

Privilege in Australia depends on the facts of each case. This section is good practice, not legal advice. Obtain legal advice early.

18. Communications

All external communications are accurate, timely, consistent and approved. Never speculate about the cause, the attacker or the data affected until facts are confirmed, and never give technical details that could help an attacker.

Audience	Prepared by	Approved by	Timing and notes
Board	Incident Executive / CRO	[CEO]	Critical: Board Risk Committee chair within [24 hours], full Board as directed. Regular updates until resolved.
Staff	Communications Lead / HR Lead	Incident Executive	What staff must do (and not do), using a safe channel. Remind staff not to discuss the incident externally or on social media.
Customers	Customer Lead / Communications Lead	[CEO] with Legal Lead review	As soon as there is something customers can act on (for example to protect accounts) or as the law requires. Include vulnerable customer support. Scripts for the contact centre.
Media and public	Communications Lead	[CEO]	Pre-approved holding statement if the incident becomes public. One spokesperson: [CEO / nominated executive] .
Regulators	Compliance and Regulatory Lead	Head of Compliance / General Counsel	Within statutory deadlines (section 19). Consistent with public statements.
Service providers and partners	Third Party Lead	Incident Executive	Need-to-know; request IOCs, logs and cooperation under the contract.
Insurer	Legal Lead	General Counsel	As the policy requires; often before engaging providers or making admissions.

Audience	Prepared by	Approved by	Timing and notes
Law enforcement and ASD	Incident Executive / Legal Lead	Incident Executive	Early (section 20).
Investors and ASX (listed entities)	Company Secretary	[Board / Disclosure Committee]	Under the continuous disclosure policy (ASX Listing Rule 3.1).

19. Regulatory and external notifications

The Compliance and Regulatory Lead assesses every possible notification and records each decision, including decisions not to notify, with reasons. Clocks run from awareness, so the time [Organisation] became aware is recorded at triage. Lodge an initial notification on time with the facts known, and update it as facts develop. The table summarises common obligations as at October 2026; delete those that do not apply and confirm current requirements.

Obligation	Applies to	Deadline and recipient
Information security incident that (a) materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or (b) has been notified to other regulators, in Australia or other jurisdictions (CPS 234 para 35)	APRA-regulated entities	APRA, as soon as possible and no later than 72 hours after becoming aware. Limb (b) means that notifying the OAIC (NDB), ASD under SOCI, or an overseas regulator also triggers an APRA notification.
Material information security control weakness that the entity expects it will not be able to remediate in a timely manner (CPS 234 para 36)	APRA-regulated entities	APRA, no later than 10 business days after becoming aware
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.	APRA-regulated entities	APRA, as soon as possible and no later than 72 hours after becoming aware

Obligation	Applies to	Deadline and recipient
Disruption to a critical operation outside tolerance (CPS 230 para 41)	APRA-regulated entities	APRA, as soon as possible and no later than 24 hours after suffering the disruption; the Board is also told, with a remediation plan
Suspected eligible data breach (<i>Privacy Act 1988</i> Part IIIC)	Entities covered by the Privacy Act	Take all reasonable steps to complete an assessment within 30 calendar days (s26WH). If eligible: statement to the OAIC (s26WK) and notification of affected individuals (s26WL) as soon as practicable
Critical cyber security incident with a significant impact on the availability of a critical infrastructure asset (SOCI Act s30BC)	Responsible entities for critical banking, superannuation, insurance and financial market infrastructure assets	ASD's ACSC within 12 hours of becoming aware; if reported orally, a written report within 84 hours of the oral report
Cyber security incident that has had, is having or is likely to have a relevant impact (availability, integrity, reliability or confidentiality) on a critical infrastructure asset (SOCI Act s30BD)	As above	ASD's ACSC within 72 hours of becoming aware; if reported orally, a written report within 48 hours of the oral report
Ransomware or cyber extortion payment made by or on behalf of the entity (<i>Cyber Security Act 2024</i> s27)	Businesses with annual turnover for the previous financial year that exceeds the threshold (\$3 million , <i>Cyber Security (Ransomware Payment Reporting) Rules 2025</i> s6), and responsible entities for SOCI Part 2B critical infrastructure assets (s26(2))	The designated Commonwealth body (Home Affairs and ASD, s8), using the ransomware payment report form on cyber.gov.au, within 72 hours of making the payment or becoming aware it was made. Civil penalty: 60 penalty units (s27(5))

Obligation	Applies to	Deadline and recipient
Reportable situation, for example a significant breach of a core obligation such as the general obligations in Corporations Act s912A, or an investigation into one continuing more than 60 days (ss912D, 912DAA; NCCP Act ss50A, 50B; the 60-day period is set by ASIC Instrument 2024/620, as described in RG 78)	AFS licensees and credit licensees	ASIC within 30 calendar days of first knowing, or being reckless as to whether, there are reasonable grounds to believe a reportable situation has arisen
Suspicious matter, for example cyber-enabled fraud or account takeover involving a designated service (AML/CTF Act s41)	AUSTRAC reporting entities	AUSTRAC within 3 business days of forming the suspicion (24 hours for terrorism financing; up to 5 business days where legal professional privilege is claimed)
Information a reasonable person would expect to have a material effect on price (ASX Listing Rule 3.1)	Listed entities	ASX immediately , unless an exception in LR 3.1A applies
Overseas regulators, payment schemes, exchanges, insurers and counterparties	As applicable	As their rules or contracts require. Note that an overseas regulator notification triggers CPS 234 para 35(b).

This summary is general information and may not be complete for your organisation. Voluntary reporting to ASD (section 20) does not replace any of these obligations. Confirm current requirements with the regulator's guidance or your legal adviser.

20. Engaging ASD, the National Cyber Security Coordinator and law enforcement

- Report cyber security incidents to ASD's Australian Cyber Security Centre as soon as they are identified, through **ReportCyber** at cyber.gov.au (Submit a report), or call the 24/7 **Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371)**. ASD can provide technical advice and assistance.
- Report cybercrime to police through ReportCyber, and in an emergency or where there is a threat to life call **000**.
- **ASD limited use obligation** (*Intelligence Services Act 2001* Part 6 Division 1A): information voluntarily provided to ASD, or acquired or prepared by ASD with the entity's consent, about a cyber security incident cannot be used for regulatory purposes, and current and former ASD staff cannot be compelled to give it in court. The protection extends to information provided by lawyers and incident response providers acting for the entity. It does not apply to information the entity later makes public.
- **National Cyber Security Coordinator** (*Cyber Security Act 2024* Part 4): an entity may voluntarily give information about a significant cyber security incident (s34: a material risk of serious prejudice to Australia's social or economic stability, defence or national security, or of serious concern to the Australian people) or about other incidents (ss 36, 39). The Coordinator and other bodies may use it only for permitted purposes, such as helping the entity respond, and not to investigate or enforce the entity's contravention of other laws, except criminal offences (ss 38 to 40). It is generally not admissible against the entity (s42).
- **Ransomware payment reports** (*Cyber Security Act 2024* Part 3) are similarly limited: they may be used only for permitted purposes (s29), not to investigate or enforce the entity's contravention of other laws, except Part 3 itself or criminal offences (ss 29, 30), and are generally not admissible against the entity (s32).
- **Limited use does not acquit mandatory reporting.** Notifications to APRA, the OAIC, ASIC, AUSTRAC and others must still be made, and regulators and law enforcement keep their own information-gathering powers. With consent, ASD can share mandatory SOCI reports with other agencies through cyber.gov.au.

21. Material service providers and third parties

- Contracts with material service providers, and other providers that hold [Organisation] 's data or connect to its systems, must require notification of security incidents affecting [Organisation] within [24 hours] (or sooner where [Organisation] 's own deadlines require), and cooperation with the investigation, including access to logs and evidence.
- An incident at a service provider is recorded and rated in [Organisation] 's register as [Organisation] 's own incident. [Organisation] remains responsible for its own notifications, even where the provider also notifies.
- Where [Organisation] relies on a provider's incident response, the provider's plan and test results are reviewed at least [annually] .
- Appendix F sets out the response to a compromised service provider.

22. Testing and exercising this Plan

CPS 234 para 26 requires APRA-regulated entities to review and test their information security response plans at least annually to ensure they remain effective and fit for purpose.

[Organisation] tests this Plan as follows:

Exercise	Who	Frequency
Executive and Board tabletop exercise on a severe but plausible scenario (for example ransomware with data theft and extortion), including ransom decisions, notifications and communications	Crisis Management Team, [Board members]	At least [annually]
Technical CIRT exercise or simulation (for example with the external responder or a red or purple team)	CIRT, IT operations, external IR provider	At least [annually]
Playbook walk-throughs (one or more of Appendices A to G)	CIRT and relevant business owners	[Quarterly] , so that each playbook is exercised at least every [2 years]

Exercise	Who	Frequency
Backup restoration test for critical systems	IT operations	At least [annually] for each critical system
Contact list and call-tree check, including out-of-band channels	Incident Manager	[Quarterly]
Joint exercise with material service providers	Third Party Lead, CIRT	[Every 2 years] or as risk requires

- Exercises should be integrated with business continuity testing under CPS 230 where scenarios overlap.
- Every exercise produces a short report with findings, which are raised as issues and tracked to closure.
- Testing of information security controls under CPS 234 paras 27 to 31 (for example penetration testing) is separate from, but should inform, these exercises.

23. Key risk indicators and reporting

The CISO reports to the executive [monthly] and to the Board Risk Committee [quarterly] on cyber incidents and on the readiness of this Plan.

Key risk indicator	Typical tolerance
Mean time to detect (from first attacker activity to detection) for High and Critical incidents	Trending down; ≤ [24 hours]
Mean time to contain High and Critical incidents (from detection)	≤ [4 hours] for Critical; ≤ [24 hours] for High
Regulatory notifications lodged on time	[100%]
Critical and High incidents with a post-incident review completed within [20 business days]	[100%]
Actions from post-incident reviews and exercises overdue	≤ [5%]; none rated High or Critical more than [90 days] overdue

Key risk indicator	Typical tolerance
Critical systems with a successful restoration test in the last 12 months	[100%]
Annual test of this Plan completed (CPS 234 para 26)	Yes
CIRT roles with a trained, named deputy	[100%]
Contact list verified in the last quarter	Yes
Material service providers with contractual incident notification terms of [24 hours] or less	[100%]

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

24. Training, roles and review

- CIRT members and deputies complete incident response training at appointment and at least [annually].
- Executives and Board members are briefed on this Plan and their decision rights at least [annually].
- All staff are trained to recognise and report suspected cyber incidents at induction and [annually].
- This Plan is reviewed at least [annually] and after any Critical or High incident or significant exercise finding. Internal Audit reviews incident response as part of its information security control assurance (CPS 234 para 32).

25. Related documents

- The RiskFA Incident & Issues Management Standard
- The RiskFA Data Breach Response Plan; the RiskFA Cyber Security Policy, the RiskFA Business Continuity Policy, the RiskFA Crisis Management Plan
- [Third Party / Material Service Provider Management Policy] , [Continuous Disclosure Policy] , [Fraud Policy] , the RiskFA Whistleblower Policy
- APRA: CPS 234 *Information Security* and CPG 234; CPS 230 *Operational Risk Management* and CPG 230
- *Cyber Security Act 2024* Parts 3 and 4; *Cyber Security (Ransomware Payment Reporting) Rules 2025*; *Security of Critical Infrastructure Act 2018* Part 2B; *Privacy Act 1988* Part IIIC; *Intelligence Services Act 2001* Part 6 Division 1A
- ASD: Ransomware Playbook, Essential Eight, *Information Security Manual*, ReportCyber; OAIC: *Data breach preparation and response*
- Standards: NIST SP 800-61 Rev. 3; NIST Cybersecurity Framework 2.0; ISO/IEC 27035-1:2023, 27035-2:2023, 27035-3 and 27035-4:2024; ISO/IEC 27001 and 27002; ISO/IEC 27037 *Guidelines for identification, collection, acquisition and preservation of digital evidence*

Appendix A. Playbook: ransomware and cyber extortion

Triggers: files encrypted, ransom note, extortion message threatening to publish stolen data, or attacker contact by email, phone or leak site. **Default severity:** Critical.

A.1 Immediate actions

1. Network-isolate affected devices; do not power them off or delete anything. Photograph ransom notes.
2. Protect backups: disconnect or lock backup systems and confirm whether they are affected.
3. Disable compromised accounts; plan a reset of privileged credentials (coordinate timing so the attacker is not tipped off before containment is ready).
4. Activate the Crisis Management Team, the external IR provider (through Legal) and the insurer.
5. Move to out-of-band communications.
6. Assume data has been stolen until proven otherwise: start the RiskFA Data Breach Response Plan.
7. Report to ASD (ReportCyber or 1300 CYBER1) and to police.
8. Start the notification checklist (Appendix L): CPS 234 72 hours, CPS 230 24 or 72 hours, SOCI 12 or 72 hours, NDB assessment.

A.2 Extortion and payment decisions

- **Government position:** the Australian Government strongly discourages paying a ransom (ASD's ACSC *Ransomware Playbook*, cyber.gov.au). Paying does not guarantee that access will be restored or that stolen data will not be sold or published, and it may lead to further attacks.
- [Organisation] 's position is that it [will not pay a ransom / will not pay except as a last resort to protect life or prevent severe customer harm] , and only with Board approval (section 7.2).
- No one may communicate with the attacker except a person authorised by the Crisis Management Team, with legal and specialist advice.
- Before any payment decision, Legal must advise on sanctions, anti-money laundering, terrorism financing and other laws, insurance terms, and whether paying would be consistent with directors' duties and the risk appetite.
- Record the decision, reasons and advice in the decision log.

A.3 If a payment is made

- Lodge a ransomware payment report (form on cyber.gov.au) within **72 hours** of making the payment or becoming aware that it was made (*Cyber Security Act 2024* s27), if [Organisation] is a reporting business entity (turnover above \$3 million, or a SOCI Part 2B responsible entity).
- The report must cover, as far as known: contact and business details of the entity that paid; the incident and its impact; the demand; the payment; and communications with the extorting entity (s27(2)).
- Payment does not end the response: eradication, recovery and data breach obligations continue.

A.4 Recovery

- Rebuild from clean images; restore from backups taken before the earliest sign of compromise; reset all credentials; monitor for re-entry.
- Monitor leak sites and dark web sources for stolen data, through the IR provider.

Appendix B. Playbook: business email compromise and payment fraud

Triggers: a fraudulent payment instruction, changed supplier or customer bank details, mailbox rules forwarding or deleting email, or reports of emails sent from a staff account without the staff member's knowledge. **Default severity:** High if money has been or may be paid; Critical above [\$X] or where customer funds are affected.

1. **Stop the money first.** Contact [Organisation]'s bank and the receiving bank immediately to request a recall or freeze. Time matters: call, do not email.
2. Reset the compromised account's password, revoke sessions and tokens, check and remove mailbox rules, forwarding and app consents, and confirm multi-factor authentication settings have not been changed.
3. Search mail logs for other affected mailboxes, phishing emails sent from the compromised account, and emails sent to customers or suppliers.
4. Warn recipients of fraudulent emails through a verified channel (a known phone number).
5. Preserve mailbox audit logs and the fraudulent emails with full headers.
6. Assess whether personal information was accessed (mailboxes often hold it) and start the RiskFA Data Breach Response Plan if so.
7. Report to police through ReportCyber, and consider an AUSTRAC suspicious matter

report where applicable.

8. Review and fix the payment control that failed (for example call-back verification of bank detail changes on a known number).

Appendix C. Playbook: data exfiltration

Triggers: evidence of data leaving the network, an extortion threat, data appearing online, unusual large transfers, or notice from a third party, ASD or the media. **Default severity:** High; Critical where large volumes of customer or sensitive data are involved.

1. Contain the exfiltration route (block destinations, disable accounts or API keys, isolate systems) while preserving evidence.
2. Start the RiskFA Data Breach Response Plan immediately. The Privacy Lead runs the NDB assessment, taking all reasonable steps to complete it within **30 calendar days** (*Privacy Act* s26WH), and notification as soon as practicable if the breach is eligible (ss 26WK, 26WL). Do not wait for the 30 days to end if serious harm is already clear.
3. Establish what data was taken, about whom, from which systems, and over what period. Identify vulnerable customers and high-risk data (for example identity documents, financial account data, health information, credentials).
4. Consider remedial action that may prevent serious harm (s26WF), such as recovering the data, confirming its deletion by a known and trusted recipient, or resetting credentials. Assurances from a malicious actor are not reliable remedial action.
5. Remember CPS 234 para 35(b): an OAIC notification also requires an APRA notification within 72 hours.
6. Help affected customers protect themselves: account monitoring, credential resets, identity document replacement support, and referral to IDCARE (a not-for-profit identity and cyber support service for Australia and New Zealand) where appropriate.
7. Monitor for publication or sale of the data through the IR provider.

Appendix D. Playbook: distributed denial of service (DDoS)

Triggers: customer-facing websites, apps, APIs or networks slowed or unavailable through traffic floods. **Default severity:** Medium; High or Critical where a critical operation is disrupted or tolerance is at risk.

1. Confirm it is an attack, not a capacity problem or a failed change.
2. Engage the DDoS protection provider or internet service provider [name, 24/7 number] to apply mitigation.
3. Invoke business continuity and customer communications if services are disrupted;

track the CPS 230 tolerance for affected critical operations.

4. Check whether the DDoS is a distraction for another attack (for example fraud or intrusion) and increase monitoring.
5. Treat any ransom demand linked to a DDoS under Appendix A.
6. Report to ASD. Consider the SOCI s30BC 12-hour obligation if the availability of a critical infrastructure asset is significantly affected.

Appendix E. Playbook: insider threat

Triggers: a staff member, contractor or service provider employee misusing access, for example taking data, sabotaging systems, committing fraud or helping an outside attacker.

Default severity: set on impact.

1. Involve the Legal Lead and HR Lead before any action that the insider could notice. Keep the group small and on a need-to-know basis.
2. Preserve evidence quietly: logs, emails, file access and device images. Use only lawful monitoring permitted by [Organisation] 's policies and workplace surveillance laws.
3. Decide, with Legal and HR, when and how to remove access. Removal of access and any interview should be coordinated.
4. Assess data impact and start the RiskFA Data Breach Response Plan if personal information is involved.
5. Consider police referral, AUSTRAC reporting and whistleblower protections (if the person has made a qualifying disclosure, handle it under the RiskFA Whistleblower Policy).
6. Review access controls, segregation of duties and monitoring for the extent of condition.

Appendix F. Playbook: compromised service provider or material service provider

Triggers: a service provider notifies a security incident, or [Organisation] detects suspicious activity coming from a provider's connection, software or update. **Default severity:** High where the provider holds [Organisation] 's data or connects to its systems; Critical where a material service provider or critical operation is affected.

1. Suspend or restrict the provider's connections, accounts and integrations where there is risk of spread, with the Incident Executive's approval.
2. Request, under the contract: what happened, when, what data and systems of [Organisation] are affected, IOCs, logs, and the provider's containment and recovery

plan. Record the time [Organisation] became aware.

3. Search [Organisation]'s environment for the IOCs and for activity from the provider's accounts.
4. Assess [Organisation]'s own notification obligations: they apply even if the provider also notifies. If personal information held by the provider is affected, [Organisation] may need to assess it under the NDB scheme (the OAIC's guidance on jointly held information applies).
5. Invoke business continuity or exit options if the provider's service will be unavailable beyond tolerance.
6. After the incident, review the provider's controls, contract terms and concentration risk.

Appendix G. Playbook: customer account takeover

Triggers: customers report unauthorised logins, changed contact details or unauthorised transactions; monitoring detects credential stuffing or unusual login patterns. **Default severity:** Medium; High or Critical where many customers or large losses are involved, or where [Organisation]'s own systems are the source of the stolen credentials.

1. Lock affected accounts, stop pending transactions, and contact affected customers through verified channels.
2. Block attack sources and apply step-up authentication or rate limits; check for changes to contact details, payees and multi-factor authentication settings.
3. Determine whether credentials came from [Organisation] (a breach) or elsewhere (reuse of passwords stolen from other sites). If from [Organisation], also run Appendix C.
4. Work with receiving financial institutions to recover funds.
5. Treat affected customers fairly, including vulnerable customers; handle disputes and complaints under the RiskFA Complaints Handling Policy and any applicable codes (for example the ePayments Code where it applies to [Organisation]).
6. Consider AUSTRAC suspicious matter reports and the NDB scheme.
7. Review authentication, fraud monitoring and customer education.

Appendix H. First-hour checklist

#	Action	Owner	Done (time)
1	Record the time [Organisation] became aware and who reported it	Incident Manager	☐
2	Open the incident record, incident log and decision log	Incident Manager / Scribe	☐
3	Call the Incident Executive; declare an initial severity	Incident Manager	☐
4	Confirm whether email and chat are safe; move to out-of-band channel if not	Technical Lead	☐
5	Take initial containment to stop active harm (isolate, disable, block); preserve evidence first where safe	Technical Lead	☐
6	Protect backups and privileged accounts	IT Operations Lead	☐
7	Select and open the relevant playbook (Appendices A to G)	Incident Manager	☐
8	Critical: activate the Crisis Management Team; inform CEO, CRO, General Counsel	Incident Executive	☐
9	Bring in the Compliance and Regulatory Lead; start Appendix L and note the earliest deadline	Incident Executive	☐
10	Personal information possibly affected: bring in the Privacy Lead and start the RiskFA Data Breach Response Plan	Incident Executive	☐
11	Critical operations affected: bring in the Business Impact Lead; invoke business continuity; start tolerance clock	Incident Executive	☐
12	Decide on engaging the external IR provider (through Legal) and notifying the insurer	Incident Executive / Legal Lead	☐
13	Tell staff who know about the incident not to discuss it outside the response team	Incident Manager	☐
14	Set the time of the next status call	Incident Manager	☐

Appendix I. Contact list template

Keep this list current (checked ☐ quarterly) and available offline. Include after-hours numbers.

Role / organisation	Name	Phone (work / mobile)	Email / other
Incident Executive (CISO) / deputy	/		
Incident Manager on-call			
CEO, CRO, General Counsel, CTO, COO			
Head of Compliance, Privacy Officer, Head of Communications			
Board Chair and Board Risk Committee Chair			
External incident response / forensics provider (retainer no.)		[24/7 number]	
External law firm			
Cyber insurer and broker (policy no. ; notification requirement)			
Crisis communications adviser			
Material service providers (security contacts)			
Bank (fraud / payment recall)			
DDoS protection / internet service provider			
ASD's ACSC: Australian Cyber Security Hotline		1300 CYBER1 (1300 292 371), 24/7	cyber.gov.au (ReportCyber)

Role / organisation	Name	Phone (work / mobile)	Email / other
Police (emergency / threat to life)		000	
APRA supervisor	[Name]	[]	[] / APRA Connect
OAIC		[]	oaic.gov.au (NDB form)
ASIC, AUSTRAC, ASX (as applicable)		[]	[]

Appendix J. Incident log template

The Scribe records every significant fact, action and item of evidence in time order. Times are in [AEST/AEDT] with the date.

Date / time	Entry (fact, action, finding)	By	Evidence item / hash / location (chain of custody)
[dd/mm/yyyy hh:mm]	[e.g. Alert received from EDR on host X]	[Name]	[Item no., SHA-256, storage location, transferred to]
[]	[]	[]	[]
[]	[]	[]	[]

Appendix K. Decision log template

Date / time	Decision	Options considered and reasons	Decided by	Advice relied on
[dd/mm/yyyy hh:mm]	[e.g. Take online banking offline]	[]	[Name, role]	[e.g. Technical Lead, Legal]
[]	[]	[]	[]	[]
[]	[]	[]	[]	[]

Appendix L. Regulator notification checklist

Complete for every Critical and High incident and any incident that may be notifiable. Record the time of awareness for each obligation, the deadline, and the decision with reasons.

Question	If yes	Deadline from awareness	Decision / lodged (time, by)
Did or could the incident materially affect us or our customers (financially or non-financially)?	APRA, CPS 234 para 35(a)	72 hours	☐
Have we notified, or will we notify, any other regulator in Australia or overseas (for example the OAIC or ASD under SOCI)?	APRA, CPS 234 para 35(b)	72 hours	☐
Is a critical operation disrupted outside its tolerance?	APRA, CPS 230 para 41	24 hours	☐
Is a material financial impact or material impact on critical operations likely (and not already notified under CPS 234)?	APRA, CPS 230 para 32	72 hours	☐
Might personal information have been accessed, disclosed or lost?	NDB assessment (s26WH); OAIC and individuals if eligible (ss 26WK, 26WL)	Assess within 30 days; notify as soon as practicable	☐
Is a SOCI critical infrastructure asset significantly affected (availability)?	ASD, SOCI s30BC	12 hours (written 84 hours after oral)	☐
Has the incident had, or is it likely to have, a relevant impact on a SOCI critical infrastructure asset (availability, integrity, reliability, confidentiality)?	ASD, SOCI s30BD	72 hours (written 48 hours after oral)	☐

Question	If yes	Deadline from awareness	Decision / lodged (time, by)
Has a ransomware or extortion payment been made by or for us?	ASD, <i>Cyber Security Act 2024</i> s27	72 hours from payment or awareness	☐
Could this be a reportable situation (for example a significant breach of s912A obligations)?	ASIC, s912DAA / NCCP s50B	30 calendar days	☐
Is there a suspicious matter involving a designated service?	AUSTRAC, AML/CTF Act s41	3 business days (24 hours for terrorism financing; up to 5 business days where legal professional privilege is claimed)	☐
Is the information price-sensitive (listed entities)?	ASX LR 3.1	Immediately	☐
Do insurance, payment scheme, overseas regulator or contract terms require notice?	As required	☐	☐
Has the incident been reported voluntarily to ASD (ReportCyber)?	Recommended in all Critical and High incidents	As soon as possible	☐

Appendix M. Post-incident review template

Section	Content
1. Summary	What happened, in two or three sentences; final severity and rating.
2. Timeline	First attacker activity, detection, awareness, containment, eradication, recovery and closure; key decisions (from the logs).
3. Impact	Customers, critical operations (against tolerance), data, financial, regulatory, reputation.
4. Root cause	How the attacker got in and why controls did not prevent or detect it sooner; root cause category and extent of condition (RiskFA Incident & Issues Management Standard).
5. Response effectiveness	What worked and what did not: detection, escalation, decision rights, playbooks, communications, service providers, evidence handling, out-of-band channels.
6. Notifications	Each notification made, its deadline and when it was lodged; any missed or late.
7. Customer outcomes	Customer communications, support and remediation, including vulnerable customers.
8. Actions	Issues raised, owners and due dates; changes to this Plan, playbooks, controls and training.
9. Sign-off	Incident Executive, CRO; reported to the executive and Board Risk Committee on [date].



[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.](#)