

Cyber Security Policy

The information security policy that sets how an organisation governs, protects, tests and reports on its information assets, aligned to current Australian regulation and ASD guidance. Ready to adapt for your organisation.

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

How to use this industry policy. Adopt the structure, terms and requirements as written, so that your organisation speaks the same language as the rest of the industry. Fill in the text in **[square brackets]** with your organisation's details, set the targets and timeframes to match your size, threat environment and risk appetite, delete obligations that do not apply to you, and approve the Policy through your governance process. Regulatory requirements are summarised as at October 2026: 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 Security Policy (information security policy)
Organisation	[Organisation name]
Document owner	[Chief Information Security Officer]
Approved by	[Board] , on the recommendation of the [Board Risk Committee]
Version / date approved	[1.0] / [date]
Review cycle	At least [annually] , and after any material change to information assets, the threat environment, regulation or the business, or after a Critical information security incident
Parent framework	[Risk Management Framework / Operational Risk Management Policy]
Supporting documents	[Information security standards and procedures] , the RiskFA Cyber Incident Response Plan, the RiskFA Incident & Issues Management Standard, the RiskFA Data Breach Response Plan, the RiskFA Quantum Risk and Post-Quantum Cryptography Standard

1. Purpose

This Policy sets the minimum requirements for protecting the **confidentiality, integrity and availability** of [Organisation] 's information assets, including those managed by related parties and third parties. It ensures that:

- the Board and management understand and govern information security risk within risk appetite;
- [Organisation] maintains an information security capability that keeps pace with changes in vulnerabilities, threats, its information assets and its business;
- information assets are identified and classified by criticality and sensitivity, and protected by controls in proportion to that classification;
- the design and operating effectiveness of controls is tested and independently assured;
- incidents are detected and responded to quickly, and regulators, customers and others are told within the required timeframes; and
- critical operations stay within their tolerance levels through severe but plausible cyber

events.

This Policy is [Organisation]'s top-level information security policy and forms part of its **information security policy framework** under APRA Prudential Standard CPS 234 *Information Security* paragraphs 18 and 19. It supports the obligations listed in section 3.

2. Scope

This Policy applies to:

- all directors, employees, contractors and consultants of [Organisation] and its subsidiaries;
- all information assets: information in any form (electronic and paper) and information technology, including software, hardware, data, cloud services, operational technology and end-user computing (for example spreadsheets and low-code tools);
- information assets managed by related parties, material service providers and other third parties, including their sub-contractors (fourth parties); and
- all locations, including remote and offshore work.

Where a related party or third party manages [Organisation]'s information assets, the requirements of this Policy apply through contract and oversight (section 19).

3. Regulatory and standards alignment

The table summarises the main requirements this Policy supports, as at October 2026. Delete those that do not apply to you.

Source	Applies to	What it requires (summary)
APRA CPS 234 <i>Information Security</i> (in force since 1 July 2019; not amended as at October 2026)	ADIs, general, life and private health insurers, RSE licensees and authorised or registered NOHCs (para 2)	Board ultimately responsible (para 13); defined roles (14); capability (15–17); policy framework (18–19); asset classification (20); controls (21–22); incident detection, response plans and annual testing (23–26); systematic control testing (27–31); internal audit (32–34); APRA notification (35–36).
APRA CPG 234 <i>Information Security</i> (June 2019)	As above (guidance, not mandatory)	APRA's guidance on how to meet CPS 234, including control testing approaches, cryptography and Board reporting.

Source	Applies to	What it requires (summary)
APRA CPS 230 <i>Operational Risk Management</i> (2026 determination, in force 1 July 2026)	APRA-regulated entities	Manage technology and data risk (para 23); maintain sound IT capability, monitor the age and health of information assets and meet CPS 234 (24); test controls for design and operating effectiveness (29); critical operations (including the systems and infrastructure that support them) and tolerance levels, including maximum data loss (35, 37); BCP testing including material service provider disruption (42–43); material service providers, including core technology services (48–55, 59–61).
ASD Essential Eight maturity model (last updated November 2023, current as at October 2026)	All organisations (guidance); mandatory only where a law, regulator or contract requires it	Eight mitigation strategies at Maturity Levels Zero to Three. Organisations set a target maturity level and implement the same level across all eight strategies before moving higher.
ASD <i>Information security manual</i> (ISM) (September 2026 release)	All organisations (guidance)	Cyber security principles and detailed controls; used as a reference library for [Organisation]'s security standards.
<i>Security of Critical Infrastructure Act 2018</i> (SOCI Act)	Responsible entities for critical infrastructure assets, including critical banking, superannuation, insurance and financial market infrastructure assets	Part 2B: report cyber security incidents to ASD (s30BC within 12 hours, s30BD within 72 hours). Part 2A: critical infrastructure risk management program (CIRMP) for assets specified in the CIRMP Rules, which include critical payment systems (critical financial market infrastructure assets in s12D(1)(i)) and critical data storage or processing assets, but not critical banking, superannuation or insurance assets as such; annual report to the relevant regulator within 90 days after the end of each financial year, approved by the board (s30AG).

Source	Applies to	What it requires (summary)
SOCI CIRMP Rules (LIN 23/006) 2023, s8 (as amended to 10 June 2026)	Entities subject to Part 2A	Minimise or eliminate material cyber and information security risks, and comply with one listed framework (for example AS ISO/IEC 27001, or the Essential Eight at Maturity Level One, or the NIST Cybersecurity Framework) or an equivalent. The enhanced CIRMP requirements added in 2026 (ss 4A and 8A–8C, including Essential Eight Maturity Level Two) apply to listed energy, water, broadcasting, domain name, freight and liquid fuel assets, not to financial market infrastructure or data storage or processing assets (s4A(1)).
<i>Cyber Security Act 2024</i> Part 3 (ss 26–27)	Businesses with annual turnover above the threshold (\$3 million: <i>Cyber Security (Ransomware Payment Reporting) Rules 2025</i> s6) and SOCI Part 2B responsible entities	Report a ransomware or cyber extortion payment to ASD within 72 hours of making it or becoming aware it was made (in force from 30 May 2025).
<i>Privacy Act 1988</i>, APP 11 and Notifiable Data Breaches scheme	APP entities	Take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure (APP 11.1); destroy or de-identify it when no longer needed (APP 11.2); reasonable steps include technical and organisational measures (APP 11.3, from 11 December 2024); assess and notify eligible data breaches.
<i>Corporations Act 2001</i> s912A(1)(a), (d) and (h)	AFS licensees (and similar obligations for credit licensees)	Provide services efficiently, honestly and fairly; have adequate financial, technological and human resources; have adequate risk management systems. The Federal Court has found that inadequate cyber security risk management breaches these obligations (see below).

Source	Applies to	What it requires (summary)
<i>Financial Accountability Regime Act 2023</i> (FAR)	ADIs, insurers and RSE licensees	An accountable person must hold senior executive responsibility for management of the entity's information management, including information technology systems (FAR (Minister) Rules 2024 s5(2)(d)), and must meet the accountability obligations in FAR Act s21.

3.1 ASIC expectations and court decisions

- *ASIC v RI Advice Group Pty Ltd* [2022] FCA 496 (5 May 2022): the Federal Court declared that RI Advice breached s912A(1)(a) and (h) by failing to have documentation and controls adequate to manage cyber security and cyber resilience risk across its authorised representative network, and ordered it to engage a cyber security expert to identify and implement further measures (ASIC 22-104MR).
- *ASIC v FIIG Securities Limited* [2026] FCA 92 (13 February 2026): FIIG admitted breaches of s912A(1)(a), (d) and (h). The failures included inadequate MFA, passwords and access controls, firewall and security software configuration, vulnerability scanning and penetration testing, patching, monitoring of threat alerts, staff awareness training, and incident response planning and testing. The Court imposed a \$2.5 million penalty and ordered an independent expert compliance program (ASIC 26-021MR).
- *ASIC v Fortnum Private Wealth Ltd* (Supreme Court of NSW, 2026): Fortnum admitted failing to have an adequate cybersecurity policy across its business and authorised representative network, adequate processes to oversee and monitor its authorised representatives' cyber resilience, adequate specialised cybersecurity expertise, and adequate cybersecurity risk management systems. The Court ordered a \$1.35 million penalty (ASIC 26-244MR).
- ASIC's open letter to licensees and directors of 8 May 2026 (26-092MR) asks licensees to act now on the cyber risk from frontier AI by strengthening the basics: protect critical assets, review user access and privileges, patch promptly, reduce attack surfaces, use defence-in-depth that assumes breach, exercise incident response and business continuity plans, and manage third-party risk.

Lesson for licensees: cyber risk management must be documented, resourced, proportionate to the size and nature of the business and the sensitivity of its data, extend to authorised representatives and service providers, and be shown to work in practice.

4. Key definitions

Definitions of CPS 234 terms follow CPS 234 paragraph 12 so that the same words mean the same thing across the industry. The remaining terms (key control, material control weakness, privileged access and phishing-resistant MFA) are this Policy's working definitions. Incident, Issue, Breach, Root cause, Critical operation and Material service provider are as defined in the RiskFA Incident & Issues Management Standard.

Term	Meaning
Information asset	Information and information technology, including software, hardware and data (both soft and hard copy).
Information security	The preservation of an information asset's confidentiality, integrity and availability.
Confidentiality / integrity / availability	Access restricted only to those authorised / completeness, accuracy and freedom from unauthorised change or usage / accessibility and usability when required.
Criticality	The potential impact of a loss of availability.
Sensitivity	The potential impact of a loss of confidentiality or integrity.
Information security capability	The totality of resources, skills and controls which provide the ability and capacity to maintain information security.
Information security control	A prevention, detection or response measure to reduce the likelihood or impact of an information security incident. This Policy uses the standard control types: preventive , detective and corrective .
Key control	A control that, on its own or with a small number of others, is relied on to keep a material risk within appetite. Key controls are tested more often and more deeply.
Information security incident	An actual or potential compromise of information security. In this Policy, a cyber security incident is an information security incident affecting information technology (the SOCI Act s12M definition applies to SOCI reporting).
Threat / vulnerability	A circumstance or event that has the potential to exploit a vulnerability / a weakness in an information asset or control that could be exploited to compromise information security.

Term	Meaning
Information security policy framework	The totality of policies, standards, guidelines and procedures pertaining to information security.
Control weakness (material)	A design or operating deficiency in a control that exposes a critical or sensitive information asset to an unacceptable risk. A material weakness that cannot be remediated in a timely manner is notifiable to APRA (section 24).
Privileged access	Access that can change systems, security settings, other users' access or large volumes of data, including administrator, service, break-glass and cloud console accounts.
Phishing-resistant MFA	Multi-factor authentication that cannot be defeated by a user entering credentials into a fake site, for example FIDO2 security keys, device-bound passkeys or smart cards (the term used in the ISM and the Essential Eight).

5. Principles

1. **The Board is ultimately responsible.** Information security is a Board-level risk, governed within risk appetite like any other material risk (CPS 234 para 13).
2. **Know what matters.** Every information asset has an owner and a classification by criticality and sensitivity. Protection follows classification.
3. **Assume breach, defend in depth.** No single control is relied on. Preventive, detective and corrective controls are layered so that a failure of one is caught by another.
4. **Least privilege and zero trust.** People and systems get only the access they need, for only as long as they need it, and every access request is verified.
5. **Secure by default and by design.** Security is built into systems, products, changes and contracts from the start, not added later.
6. **Do the basics well, everywhere.** The Essential Eight is the minimum baseline, implemented consistently across all eight strategies to the target maturity level.
7. **Keep controls current.** Controls are monitored, tested and adjusted as threats, vulnerabilities, technology and the business change (CPS 234 para 17), so that [Organisation] stays within risk appetite.
8. **Third parties are part of our perimeter.** Information assets managed by others meet the same standard, and we verify it.
9. **Detect and respond fast.** We plan for incidents that could plausibly occur, rehearse the plans, and meet every notification clock.
10. **Prove it.** Controls are tested for design and operating effectiveness by people independent of their operation, and results are reported honestly.

6. Three lines of accountability

Line	Who	Responsibilities
First line	Business units, asset owners, Technology, the security operations function, control owners	Own information security risk in their areas; classify and protect assets; operate controls; perform control self-assessment; fix weaknesses; report incidents.
Second line	[CISO office, where independent of IT delivery], Risk and Compliance	Own this Policy and the security standards; set the control baseline; challenge risk assessments and exceptions; run or oversee the systematic testing program; monitor metrics and risk appetite; report to management and the Board.
Third line	Internal Audit	Independently review the design and operating effectiveness of information security controls, including those maintained by related parties and third parties (CPS 234 paras 32–34).

Where the CISO reports to the Chief Technology Officer, decide whether the CISO office is first or second line and record it. If it is first line, Risk must provide independent challenge of information security risk. Testing must still be conducted by functionally independent specialists (CPS 234 para 30).

7. Governance, roles and responsibilities

CPS 234 paragraph 14 requires the information security roles of the Board, senior management, governing bodies and individuals to be clearly defined. [Organisation] defines them as follows.

Role	Responsibilities
Board	Ultimately responsible for information security (CPS 234 para 13). Approves this Policy and the information security risk appetite; ensures the capability is commensurate with the size and extent of threats; receives regular reporting on threats, control effectiveness, testing, incidents and remediation; is told of material incidents and material control weaknesses; challenges management on whether resources are adequate.

Role	Responsibilities
Board Risk Committee	Recommends this Policy to the Board; oversees information security risk against appetite, the testing program, exceptions outside appetite, and notifications to APRA and other regulators.
Board Audit Committee	Oversees internal audit coverage of information security controls and the closure of audit issues.
CEO and executive team	Provide adequate resources; foster a security-aware culture; own information security risk and controls in their areas.
Accountable person for information management (FAR, where applicable)	Holds senior executive responsibility for management of information management, including information technology systems (FAR (Minister) Rules 2024 s5(2)(d)); takes reasonable steps to prevent matters that would adversely affect the entity's prudential standing or reputation (FAR Act s21). Usually the [Chief Technology Officer / Chief Information Officer] .
Chief Information Security Officer (CISO)	Owns this Policy and the security standards; leads the information security capability and strategy; maintains the threat assessment and control baseline; reports to the executive and the Board at least [quarterly] ; decides on security exceptions within delegation; leads response to information security incidents with the incident owner; advises on APRA, ASD and other notifications.
Chief Technology Officer	Designs, builds and runs technology in line with this Policy; owns most technical controls; monitors the age and health of information assets (CPS 230 para 24); funds and delivers remediation.
Chief Risk Officer (CRO)	Ensures information security risk is integrated with the risk management framework and risk appetite; provides independent challenge; approves risk acceptances outside appetite for Board Risk Committee endorsement.
Head of Compliance / General Counsel	Assess and make regulatory notifications (APRA, ASIC, OAIC, ASD); manage legal privilege; advise on privacy obligations.
Chief Privacy Officer / Privacy Officer	Ensures APP 11 obligations are met; leads assessment of suspected eligible data breaches.
Information asset owner	A senior manager accountable for an information asset: classifies it, approves access, accepts residual risk within delegation and ensures controls are in place.

Role	Responsibilities
Control owner	Operates and evidences assigned controls; reports failures; supports testing.
Third-party / service provider owner	Manages security requirements, assessments and oversight for each arrangement (section 19).
All staff and contractors	Follow this Policy and the [Acceptable Use Standard] ; complete training; protect credentials; report suspected incidents, phishing and weaknesses immediately.

8. Information security capability

[Organisation] must maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity (CPS 234 para 15). To do this, **[Organisation]** :

- maintains a **threat assessment**, updated at least **[annually]** and when threat intelligence changes, covering the actors, techniques and scenarios most relevant to its business, customers and critical operations;
- maintains an **information security strategy** and multi-year roadmap, approved by the **[Board Risk Committee]** , that closes gaps between current and target capability (including the Essential Eight target maturity level);
- ensures enough **skilled people** (internal or contracted), with succession for key roles and no single point of dependency;
- subscribes to threat intelligence, including ASD advisories and alerts, and acts on relevant items within **[timeframe]** ;
- assesses the information security capability of related parties and third parties that manage its information assets, in proportion to the potential consequences of an incident (CPS 234 para 16); and
- actively updates its capability for changes in vulnerabilities and threats, including from changes to its information assets or business environment such as new products, cloud services, mergers, offshoring and new technology such as AI (CPS 234 para 17; CPS 230 para 25).

9. Information security policy framework

The information security policy framework must be commensurate with [Organisation] 's exposure to vulnerabilities and threats, and give direction on the responsibilities of all parties who must maintain information security, including staff, contractors, related parties, third parties and customers (CPS 234 paras 18–19).

Level	Document	Approved by
Policy	This Cyber Security Policy	[Board]
Standards	Mandatory technical and process requirements, for example: [Access Control Standard] , [Cryptography and Key Management Standard] , [Secure Configuration Standard] , [Vulnerability and Patch Management Standard] , [Logging and Monitoring Standard] , [Secure Development Standard] , [Third-Party Security Standard] , [Backup Standard] , [Acceptable Use Standard]	[CISO]
Procedures and guidelines	How-to steps and good-practice guidance	[Control owners / function heads]
Plans	The RiskFA Cyber Incident Response Plan (the information security response plan) and playbooks	[Executive / Board Risk Committee]

Standards are reviewed at least [annually] and after material changes. They draw on the ISM, CPG 234, ASD hardening guidance and recognised standards such as AS ISO/IEC 27001 and AS ISO/IEC 27002, and the NIST Cybersecurity Framework.

10. Information asset identification and classification

[Organisation] must classify its information assets, including those managed by related parties and third parties, **by criticality and sensitivity**. The classification must reflect the degree to which an information security incident affecting the asset could affect, financially or non-financially, [Organisation] or the interests of depositors, policyholders, beneficiaries or other customers (CPS 234 para 20).

- An **information asset register** records every material information asset: owner, description, location (including cloud region and offshore), the service provider (if any), the critical operations it supports, criticality and sensitivity ratings, and the date last reviewed.

- Assets are discovered automatically where possible (for example network scanning and cloud inventory at least [fortnightly], consistent with Essential Eight asset discovery), and reconciled with the register at least [quarterly].
- Criticality is set using the critical operations register and tolerance levels (CPS 230 paras 33 and 37), including the maximum data loss tolerated.
- Sensitivity is set using the classification scheme in Appendix B. Information is labelled with its sensitivity, and handled accordingly.
- Classification is reviewed at least [annually], and when an asset, its use, or the data it holds changes significantly.
- Assets are managed across their life-cycle, from planning and design to decommissioning and secure disposal.

11. Implementation of controls

[Organisation] must have information security controls that protect its information assets, including those managed by related parties and third parties, and that are implemented in a timely manner and commensurate with: vulnerabilities and threats; the criticality and sensitivity of the assets; the stage of the asset's life-cycle; and the potential consequences of an incident (CPS 234 para 21). Controls are designed, implemented and embedded in line with risk appetite and are monitored and tested for design and operating effectiveness (CPS 230 paras 28–29).

11.1 Control baseline and Essential Eight target

- The CISO maintains a **control baseline** (Appendix A) that maps each control to the Essential Eight, the CPS 234 paragraphs and the relevant ISM guideline, with an owner, control type (preventive, detective, corrective), whether it is a key control, and its testing frequency.
- [Organisation] 's Essential Eight target is **[Maturity Level Two]** across all eight strategies for the corporate environment, and **[Maturity Level Three]** for systems that support critical operations or hold Highly Confidential information. ASD recommends reaching the same maturity level across all eight strategies before moving higher.
- The Essential Eight is a minimum set of preventive measures for internet-connected IT networks. It does not address every threat, and is not designed for operational technology or enterprise mobility. [Organisation] adds controls from the ISM and other standards where its risk assessment requires.
- Where [Organisation] is subject to the SOCI CIRMP Rules, it records which framework it complies with under Rules s8(4) or (5) (for example the Essential Eight at no less than Maturity Level One).
- Controls are prioritised on risk: critical and internet-facing assets first.

11.2 Control design and the control environment

- Every material information security risk in the risk register is linked to its key controls. Controls are rated effective, partly effective or ineffective based on testing (section 22).
- Controls are monitored continuously where practicable (for example automated configuration, patch and MFA coverage checks) and the results are reported against risk appetite metrics (section 26). When monitoring shows a control is drifting outside its target, the control owner acts and the change is recorded.
- Control gaps and weaknesses are raised as issues and managed under the RiskFA Incident & Issues Management Standard until remediated, and stay in the operational risk profile until fixed (CPS 230 para 30).
- Where information assets are managed by a related party or third party, [Organisation] evaluates the design of that party's controls that protect its assets (CPS 234 para 22; section 19).

12. Identity and access management

12.1 All users

- Every user has a unique, named identity. Shared accounts are prohibited unless approved as an exception with compensating controls.
- Access is granted on least privilege and need-to-know, approved by the information asset owner, and provisioned through [the identity governance tool] wherever possible.
- Joiners, movers and leavers: access is removed on the last day of employment or engagement (immediately for terminations), and changed on role change.
- Access to systems holding Confidential or higher information is reviewed at least [six-monthly], and privileged access at least [quarterly].
- Password and passphrase rules follow the ISM. Credentials are never shared, and compromised credentials are reset immediately.
- Customer-facing authentication is risk-based. Higher-risk customer and member activities (for example changes to contact or bank details, withdrawals, rollovers and benefit transfers) require MFA or an equivalent control, with alternatives for customers who cannot use digital channels.

12.2 Multi-factor authentication

- MFA is required for: all remote access; all access to [Organisation]'s and third-party online services that process, store or communicate sensitive data; all privileged access; all users of systems; and access to email, cloud consoles and identity providers.
- MFA used for staff access to online services and systems is **phishing-resistant** (required at Essential Eight Maturity Level Two). SMS and voice codes are not used for staff, and are phased out for customers where phishing-resistant options are available.
- Customers of online services are offered a phishing-resistant MFA option.
- Successful and unsuccessful MFA events are centrally logged and monitored.

APRA wrote to all RSE licensees on 10 June 2025 after credential-stuffing attacks, setting the expectation that MFA or equivalent controls apply to all high-risk member activities (such as changing member details, withdrawals, benefit payments, transfers, rollovers and investment switching) and to all administrative and privileged access. Each RSE licensee was asked to self-assess its authentication controls and, by 31 August 2025, notify APRA of any material control weakness (or explain why an identified issue is not material) and assess and notify any breach. Other APRA-regulated entities should treat this as a clear signal of APRA's expectations under CPS 234.

12.3 Privileged access

- Privileged access is requested, validated and approved before it is granted, and is disabled after [12 months] unless revalidated, and after [45 days] of inactivity (Essential Eight Maturity Level Two).
- Privileged users have a separate, dedicated privileged account used only for privileged duties. Privileged accounts cannot access the internet, email or web services unless explicitly authorised and limited.
- Administration is done from separate privileged operating environments and through jump servers or a privileged access management tool. Just-in-time access is used for the most sensitive systems where practicable.
- Credentials for break-glass, local administrator and service accounts are long, unique, unpredictable and managed in a vault.
- Privileged access events, and privileged account and security group changes, are centrally logged, protected from change, and reviewed.

13. Secure configuration, patching and vulnerability management

13.1 Secure configuration and hardening

- Systems are built from approved, hardened baselines using ASD and vendor hardening guidance (the most restrictive applies when they conflict). Deviations are exceptions.
- **Application control** restricts execution to an organisation-approved set on workstations and internet-facing servers, and rulesets are validated at least [annually].
- **Microsoft Office macros** are disabled for users without a demonstrated business need; macros from the internet are blocked; users cannot change macro security settings.
- **User application hardening**: web browsers, office productivity suites and PDF software are hardened and users cannot change their security settings; unneeded features are removed.
- Configuration drift is detected automatically and corrected within [timeframe].
- Unsupported (end-of-life) operating systems and applications are removed or replaced. Any that remain are exceptions with compensating controls and a retirement date.

13.2 Vulnerability management

- Vulnerability scanning with an up-to-date database runs at least daily for online services and internet-facing systems, weekly for office productivity suites, browsers, email clients, PDF software and security products, and fortnightly for other applications and internal systems (Essential Eight).
- Vulnerabilities are rated using vendor severity, exploit availability (including known-exploited lists), exposure and asset classification.
- Threat intelligence and ASD alerts about actively exploited vulnerabilities trigger an emergency response.
- Overdue vulnerabilities are reported to the CISO and asset owner, and those that cannot be fixed in time go through the exception process (section 25).

13.3 Patch timeframes

Patches, updates or other vendor mitigations are applied within these timeframes from release. They match Essential Eight Maturity Level Two; tighten them for Maturity Level Three systems.

Asset	Critical, or working exploit exists	Other
Online services, and operating systems of internet-facing servers and network devices	[48 hours]	[2 weeks]
Office productivity suites, web browsers and extensions, email clients, PDF software, security products	[2 weeks] (ML3: [48 hours])	[2 weeks]
Other applications	[1 month]	[1 month]
Operating systems of workstations, non-internet-facing servers and non-internet-facing network devices	[1 month] (ML3: [48 hours])	[1 month]
Drivers and firmware (an Essential Eight requirement from ML3)	[1 month] (ML3: [48 hours])	[1 month]

ASIC's 8 May 2026 open letter warns that AI is speeding up vulnerability discovery and exploitation. Treat these timeframes as maximums, not targets.

14. Logging, monitoring and detection

[Organisation] must have robust mechanisms to detect and respond to information security incidents in a timely manner (CPS 234 para 23).

- Security-relevant events are logged centrally, including authentication and MFA events, privileged activity, account and group changes, application control events, command-line and PowerShell events, internet-facing server logs, cloud control-plane events, and security tool alerts.
- Logs are synchronised to a reliable time source, protected from unauthorised change or deletion, and kept for at least [18 months] ([7 years] where required for records).
- A security operations function (in-house or managed) monitors alerts [24 hours a day, 7 days a week] for critical systems, using defined use cases mapped to the threat assessment.
- Cyber security events are analysed in a timely manner to identify incidents. Incidents are reported to the CISO or a delegate as soon as possible, and the RiskFA Cyber Incident Response Plan is enacted.
- Proactive threat hunting is carried out at least [quarterly], using current threat intelligence.
- Detection coverage is reviewed at least [annually] against the threat assessment, and after every significant incident.
- Data loss prevention and user activity monitoring are used for Highly Confidential information, consistent with privacy and workplace surveillance laws.

15. Network, endpoint and email security

15.1 Network security

- Networks are segmented by trust and function, so that a compromise in one zone cannot spread freely. Critical systems, privileged environments, backups and payment systems are in protected segments.
- Traffic between zones and to the internet is denied by default and allowed only by approved rules. Firewall rules are reviewed at least [six-monthly].
- The internet-facing attack surface is kept to a minimum, inventoried, and scanned. Administrative interfaces are never exposed directly to the internet.
- Remote access uses approved, MFA-protected services with device health checks.
- Wireless, DNS and web traffic are protected and filtered, and encrypted protocols are used.
- Protection against denial-of-service attacks is in place for critical customer-facing services.

15.2 Endpoint security

- All endpoints (laptops, desktops, servers, mobile devices) are enrolled in management, encrypted, hardened and patched, and run endpoint detection and response.
- Personal devices may access [Organisation] information only through approved, managed containers or virtual desktops.
- Removable media is blocked by default, and allowed only by exception with encryption.

15.3 Email and web security

- Email is filtered for malware, phishing and impersonation. Attachments and links are scanned or detonated before delivery.
- Sender authentication (SPF, DKIM and DMARC at enforcement) protects [Organisation]'s domains from spoofing.
- External emails are clearly tagged. Staff can report suspicious emails in one click, and reports are triaged promptly.
- Web access is filtered, and access to newly registered, malicious and uncategorised sites is blocked.

16. Backup and recovery

- Backups of data, applications and settings are performed and retained in line with business criticality and business continuity requirements, including the maximum data loss tolerance for each critical operation (CPS 230 para 37(b)).
- Backups are synchronised so that systems can be restored to a common point in time.
- Backups are retained in a secure and resilient manner: at least one copy is immutable or offline and logically separated from production identity systems, so that ransomware or a compromised administrator cannot delete or encrypt it.
- Unprivileged accounts cannot access backups belonging to other accounts, and cannot modify or delete backups. Privileged accounts other than backup administrators cannot access backups belonging to other accounts, and cannot modify or delete backups (Essential Eight Maturity Level Two). At Maturity Level Three, backup administrators also cannot modify or delete backups during their retention period.
- Restoration to a common point in time is tested as part of disaster recovery exercises at least [annually] for each critical operation, and the results are compared against tolerance levels.
- Recovery plans assume that a cyber attack may make primary systems and recent backups untrustworthy, and include clean-room or isolated recovery for critical systems.
- Backup and recovery are included in the BCP testing program, including severe but plausible cyber scenarios and disruption at material service providers (CPS 230 paras 42–43).

17. Data security, encryption and key management

17.1 Data protection

- Information is handled according to its sensitivity label (Appendix B), including where it may be stored, who may access it and how it may be shared.
- Personal information is protected under APP 11 using technical and organisational measures, collected only where needed, and destroyed or de-identified when no longer needed for any permitted purpose (APP 11.2), subject to record-keeping laws.
- Production data containing personal or Confidential information is not used in development or test environments unless masked or de-identified, or approved as an exception.
- Data stored, processed or accessed offshore is identified in the information asset register, and the risks are assessed before it moves (see section 19 for APRA notification).
- Media and equipment are sanitised or destroyed securely at end of life, with evidence kept.

17.2 Encryption

- Confidential and Highly Confidential information is encrypted in transit and at rest, including on endpoints, removable media, backups and in cloud services.
- Only approved algorithms, key lengths and protocols are used, in line with the ISM *Guidelines for cryptography*. Weak and deprecated protocols are disabled.
- [Organisation] keeps an inventory of where and how cryptography is used (a cryptographic inventory), to support crypto-agility.

17.3 Key management

- Cryptographic keys are generated, stored, rotated, backed up and destroyed under the [Cryptography and Key Management Standard], using hardware security modules or managed key services for high-value keys.
- Duties are separated so that no single person can access both encrypted data and its keys without oversight.
- Keys for the most sensitive data held in the cloud are controlled by [Organisation] where practicable.
- Certificates are inventoried, monitored for expiry and renewed automatically where possible.

17.4 Post-quantum cryptography

A future cryptographically relevant quantum computer could break today's public-key cryptography, and data stolen now could be decrypted later. ASD's ISM recommends ceasing use of traditional asymmetric cryptography (such as RSA, Diffie-Hellman, ECDH and ECDSA) by the end of 2030 and moving to ASD-approved post-quantum algorithms. [Organisation] plans and manages this transition under the RiskFA Quantum Risk and Post-Quantum Cryptography Standard, starting with the cryptographic inventory and long-lived sensitive data.

18. Secure development and change

- Security requirements, threat modelling and privacy impact assessment are part of the design of every new system, product, significant change and AI use case.
- Software is developed under the [Secure Development Standard], including secure coding practices, peer code review, automated code and dependency scanning, secrets scanning and a software bill of materials for key applications.
- Separate development, test and production environments are kept, and developers do not have standing access to production.
- Changes to production follow the [Change Management Standard]: risk-assessed, tested, approved, scheduled and reversible. Emergency changes are reviewed after the event.
- High-risk and internet-facing applications are security tested (for example penetration testing) before go-live and after significant change.
- Systems are not put into production with known High or Critical vulnerabilities unless approved as an exception.
- Off-the-shelf and open-source software is checked for supported status, known vulnerabilities and supply chain risk before use.
- Low-code tools, end-user computing and AI tools that handle Confidential information are inventoried and controlled in proportion to their risk.

19. Cloud, third-party and material service provider security

Information assets managed by related parties and third parties are protected to the same standard as [Organisation]'s own. This section works with the [Service Provider Management Policy] required by CPS 230 paragraph 46.

19.1 Before entering into an arrangement

- Every arrangement involving [Organisation] 's information assets is risk-assessed, based on the classification of the assets and the potential consequences of an incident.
- [Organisation] assesses the provider's information security capability (CPS 234 para 16) and evaluates the design of its controls that protect [Organisation] 's assets (CPS 234 para 22), using questionnaires, independent assurance reports (for example ISAE 3402 / ASAE 3402, SOC 2 or ISO/IEC 27001 certification with a relevant scope), and on-site or technical testing for the highest-risk arrangements.
- Due diligence for material arrangements includes the provider's ability to provide the service on an ongoing basis, and risks from geographic location and concentration, including fourth parties (CPS 230 paras 47 and 52).
- Core technology services providers are classified as material service providers unless [Organisation] can justify otherwise (CPS 230 para 49(d)).

19.2 Contract requirements

Agreements must, in proportion to the risk, include:

- compliance with this Policy or equivalent controls, and with applicable law;
- ownership and control of data, data location (including offshore), and return or destruction of data on exit;
- notification of information security incidents affecting [Organisation] within [24 hours] (shorter for critical services), so that [Organisation] can meet its 72-hour, 24-hour and 12-hour notification clocks;
- notification of material sub-contractors the provider relies on (CPS 230 para 53(d)) and responsibility for their failures (para 53(e));
- audit and testing rights for [Organisation] , and access and on-site visit rights for APRA (CPS 230 para 54);
- security testing and reporting obligations, and remediation of findings; and
- business continuity, exit and termination provisions.

19.3 Ongoing oversight

- Each arrangement has an owner who monitors security performance, including the effectiveness of controls (CPS 230 para 59(b)).
- Security reassessments are performed at least [annually] for material service providers and arrangements involving Highly Confidential information, and every [2–3 years] for others.
- Where [Organisation] relies on the provider's control testing, it assesses whether the nature and frequency of that testing is adequate (CPS 234 para 28).
- APRA is notified within 20 business days of entering into or materially changing an agreement for a service relied on to undertake a critical operation, and before entering into any material offshoring arrangement, including where data will be located offshore (CPS 230 para 60).
- Authorised representatives, brokers and other distribution partners who handle [Organisation]'s customer data are subject to minimum cyber security requirements and oversight, proportionate to the data they hold (see *ASIC v RI Advice*).

19.4 Cloud services

- Cloud services are used only after a security and risk assessment, and on approved platforms and regions.
- The shared responsibility model is documented for each service, so that it is clear which controls the provider operates and which [Organisation] operates.
- Cloud configuration is managed as code where practicable and continuously checked against approved baselines (cloud security posture management).
- Cloud administrator accounts, root accounts and identity providers are treated as privileged access with the strongest controls.

20. Security awareness, culture and personnel security

- All staff and contractors complete security and privacy awareness training at induction and at least [annually], covering phishing, social engineering, credential protection, data handling, AI tools, and how to report incidents.
- Role-based training is given to privileged users, developers, the security team, executives and the Board.
- Phishing simulations run at least [quarterly]. Repeat failures lead to further training, not blame.
- Background and reference checks are proportionate to the role and the sensitivity of access. Roles with privileged or Highly Confidential access receive enhanced screening.
- Staff must report a suspected incident or weakness immediately, without fear of penalty for reports made in good faith.
- Breaches of this Policy are managed under the RiskFA Consequence Management Framework.

21. Information security incident management

[Organisation] must have robust mechanisms to detect and respond to incidents in a timely manner, and must maintain information security response plans for incidents that could plausibly occur (CPS 234 paras 23–24). The response plans must cover all stages of an incident, from detection to post-incident review, and escalation and reporting to the Board, other governing bodies and individuals responsible for incident management and oversight (para 25).

- The **RiskFA Cyber Incident Response Plan** is [Organisation]'s information security response plan. It includes playbooks for at least: ransomware and extortion, business email compromise, data theft, credential stuffing and account takeover, insider threat, denial of service, compromise of a material service provider, and destructive attacks.
- Every information security incident is recorded, rated, escalated, investigated to root cause and closed under the **RiskFA Incident & Issues Management Standard**, using the standard rating scale (Critical, High, Medium, Low).
- Evidence is preserved from the start. Forensic and legal support are arranged in advance.
- Decisions on ransomware or extortion payments are reserved for the [Board / CEO], on legal advice, and any payment is reported through the cyber.gov.au ransomware payment report form within 72 hours where the *Cyber Security Act 2024* applies (section 24).

- Response plans are reviewed and tested **at least annually** to ensure they remain effective and fit for purpose (CPS 234 para 26), through exercises that include the executive and, at least every **[2 years]**, the Board.
- Lessons learned from incidents, near misses and exercises update the threat assessment, controls and plans.

22. Testing control effectiveness

[Organisation] must test the effectiveness of its information security controls through a **systematic testing program** (CPS 234 para 27). The nature and frequency of testing must be commensurate with: the rate at which vulnerabilities and threats change; the criticality and sensitivity of the asset; the consequences of an incident; the risks of exposure to environments where **[Organisation]** cannot enforce its policies (untrusted environments); and the materiality and frequency of change to the asset.

22.1 The testing program

Test type	What it covers	Typical minimum frequency
Control design and operating effectiveness testing	Key controls in the control baseline, tested against evidence over a period	[Annually] for key controls on critical assets; [every 2 years] for others
Automated control monitoring	MFA, patch, configuration, endpoint, backup and logging coverage	[Continuous / daily]
Vulnerability scanning	All assets	Daily to fortnightly (section 13.2)
Penetration testing	Internet-facing systems, critical applications, cloud environments, internal network	[Annually] and after significant change
Red team or threat-led testing	Detection and response against realistic attack scenarios	[Every 2 years] for larger entities, or as directed
Essential Eight assessment	Maturity against the target level for each strategy, using ASD's assessment process	[Annually]
Incident response exercise	Response plans and playbooks (CPS 234 para 26)	At least annually
Backup restoration and disaster recovery test	Restoration within tolerance levels	At least annually for each critical operation
Phishing simulation	Staff behaviour	[Quarterly]
Third-party assurance review	Provider controls and their testing (CPS 234 para 28)	Section 19.3

22.2 Requirements

- Testing is performed by appropriately skilled and **functionally independent** specialists (CPS 234 para 30). Independence means the tester does not design or operate the control being tested.
- Test findings are rated, recorded as issues and remediated under the RiskFA Incident & Issues Management Standard. Remediation is retested before closure.
- Testing results that identify control deficiencies that **cannot be remediated in a timely manner** are escalated and reported to the Board or senior management (CPS 234 para 29), and assessed for APRA notification (para 36).
- The sufficiency of the testing program is reviewed **at least annually**, or when there is a material change to information assets or the business environment (CPS 234 para 31). The review is reported to the [Board Risk Committee].
- Results of control testing are reported to senior management, and gaps are rectified in a timely manner (CPS 230 para 29).

23. Internal audit

- Internal audit activities include a review of the **design and operating effectiveness** of information security controls, including those maintained by related parties and third parties (information security control assurance) (CPS 234 para 32).
- Internal audit uses personnel appropriately skilled in providing such assurance, using co-sourced specialists where needed (CPS 234 para 33).
- Where an incident affecting assets managed by a related party or third party could materially affect [Organisation] or its customers, and internal audit intends to rely on that party's control assurance, internal audit assesses the quality of that assurance (CPS 234 para 34).
- Internal audit's information security coverage is set out in a risk-based plan approved by the [Board Audit Committee], and covers this Policy, the testing program and the remediation of findings.

24. Notifications to APRA and other parties

Notification decisions are made under the RiskFA Incident & Issues Management Standard and the RiskFA Cyber Incident Response Plan. The table summarises information security notifications as at October 2026. Clocks run from when [Organisation] becomes aware, not from the end of an investigation.

Obligation	Applies to	When to notify
------------	------------	----------------

Obligation	Applies to	When to notify
Information security incident that 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 that has been notified to other regulators in Australia or overseas (CPS 234 para 35)	APRA-regulated entities	APRA, as soon as possible and no later than 72 hours after becoming aware
Material information security control weakness the entity expects it will not be able to remediate in a timely manner (CPS 234 para 36)	APRA-regulated entities	APRA, as soon as possible and no later than 10 business days after becoming aware
Operational risk incident likely to have a material financial impact or a material impact on critical operations (CPS 230 para 32). An incident already notified under CPS 234 does not need to be notified again (fn 11).	APRA-regulated entities	APRA, no later than 72 hours after becoming aware
Disruption to a critical operation outside tolerance (CPS 230 para 41)	APRA-regulated entities	APRA, no later than 24 hours after the disruption
Cyber security incident with a significant impact (s30BC) or relevant impact (s30BD) 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

Obligation	Applies to	When to notify
Suspected eligible data breach (Privacy Act Part IIIC)	APP entities	Assess within 30 calendar days ; if eligible, notify the OAIC and affected individuals as soon as practicable (see the RiskFA Data Breach Response Plan)
Reportable situation, for example a significant breach of s912A arising from cyber security failures (Corporations Act s912DAA)	AFS licensees (and credit licensees under the NCCP Act)	ASIC within 30 calendar days (see the RiskFA Incident & Issues Management Standard)
FAR notifiable events (FAR Act s31, s32)	Accountable entities	APRA and ASIC within 30 days

Reporting cyber security incidents to ASD voluntarily is encouraged even where no law requires it, and is part of the Essential Eight Maturity Level Two requirements. Check insurance policy notification terms as well.

25. Exceptions and risk acceptance

Exceptions should be rare, limited in scope and time, and supported by compensating controls. ASD's Essential Eight guidance expects exceptions to be documented, approved through an appropriate process, minimised, and regularly reviewed.

- Every exception from this Policy or a security standard is recorded in the **exception register** with: the requirement not met, the reason, the assets and users affected, the residual risk rating, compensating controls, the owner, and an expiry date of no more than **[12 months]**.
- Approvals: Low and Medium residual risk, the **[CISO]**; High, the **[CISO and CRO]** with the accountable executive; Critical or outside risk appetite, the **[Board Risk Committee]** on the CRO's recommendation.
- Exceptions are reviewed before expiry. An expired exception is a breach of this Policy and is reported.
- Formal risk acceptance follows the RiskFA Incident & Issues Management Standard. Risk acceptance can never be used to accept a breach of law.
- An exception does not remove the need to assess whether the weakness is a material control weakness notifiable to APRA under CPS 234 paragraph 36.

26. Risk appetite, metrics and reporting

- The Board sets information security risk appetite statements, supported by measurable limits and key risk indicators (KRIs) (Appendix C).
- The CISO reports to the executive [monthly] and to the [Board Risk Committee] at least [quarterly] on: the threat environment; KRIs against limits; Essential Eight maturity against target; control testing results; material incidents and near misses; notifications; material weaknesses and remediation; exceptions; and third-party security.
- Any KRI outside its limit is escalated with an action plan. A breach of risk appetite is reported to the Board.
- The Board receives at least [annually] a report on the overall state of information security, the adequacy of the capability and resources, and the strategy.
- Reports focus on risk and trends, in plain language, not on volumes of technical data.

27. Compliance, review and related documents

27.1 Compliance with this Policy

Compliance with this Policy is mandatory. Breaches are recorded as incidents, managed under the RiskFA Incident & Issues Management Standard and the RiskFA Consequence Management Framework, and considered in performance and remuneration outcomes under the RiskFA Remuneration Policy (CPS 511 where it applies). The CISO may direct the immediate removal of access or isolation of a system to protect information assets.

27.2 Review

The CISO reviews this Policy at least [annually], and after any material change to the threat environment, information assets, the business or regulation, or after a Critical incident. The Board approves material changes.

27.3 Related documents

- RiskFA Risk Management Framework; RiskFA Incident & Issues Management Standard; RiskFA Cyber Incident Response Plan; RiskFA Data Breach Response Plan; RiskFA Quantum Risk and Post-Quantum Cryptography Standard
- [Service Provider Management Policy] , the RiskFA Business Continuity Policy, [Privacy Policy] , [Acceptable Use Standard] and the security standards listed in section 9
- APRA: CPS 234 and CPG 234, CPS 230 and CPG 230, CPS 220 / SPS 220, CPS 511
- ASD: Essential Eight maturity model and FAQ; *Information security manual*; *Strategies to mitigate cyber security incidents*; *Planning for post-quantum cryptography*
- Legislation: SOCI Act and CIRMP Rules; *Cyber Security Act 2024*; *Privacy Act 1988* (APP 11 and Part IIIC); *Corporations Act 2001* s912A; FAR Act
- ASIC: RG 78 *Breach reporting by AFS licensees and credit licensees*; ASIC cyber resilience publications and the open letter of 8 May 2026
- Standards: AS ISO/IEC 27001 and AS ISO/IEC 27002, AS ISO 31000 *Risk management*, ISO/IEC 27035 *Information security incident management*, ISO 22301 *Business continuity*, NIST Cybersecurity Framework

Appendix A. Control baseline: Essential Eight and CPS 234 mapping

Key controls are marked. Adapt the targets to your Essential Eight target maturity level. Type: P = preventive, D = detective, C = corrective.

Control area	Minimum control (target [ML2])	Type	Essential Eight	CPS 234	Policy section
Asset management	Information asset register; automated asset discovery at least fortnightly; classification by criticality and sensitivity	P	Supports Patch applications / Patch OS	Para 20	10
Application control (key)	Approved set only on workstations and internet-facing servers; Microsoft recommended blocklist; annual ruleset validation	P	Application control	Para 21	13.1

Control area	Minimum control (target [ML2])	Type	Essential Eight	CPS 234	Policy section
Patching: applications (key)	Scanning and patch timeframes in section 13.3; remove unsupported applications	P/C	Patch applications	Para 21	13.2–13.3
Macros	Disabled unless business need; internet macros blocked; users cannot change settings	P	Restrict Microsoft Office macros	Para 21	13.1
Application hardening	Browsers, Office and PDF software hardened; settings locked; PowerShell and command-line events logged	P/D	User application hardening	Para 21	13.1, 14
Privileged access (key)	Validated, time-limited, separate accounts and environments; jump servers; vaulted credentials; events logged	P/D	Restrict administrative privileges	Para 21	12.3
Patching: operating systems (key)	Scanning and patch timeframes in section 13.3; replace unsupported operating systems	P/C	Patch operating systems	Para 21	13.2–13.3
MFA (key)	Phishing-resistant MFA for staff on online services and systems; MFA for privileged access and high-risk customer activities; events logged	P/D	Multi-factor authentication	Para 21	12.2
Backups (key)	Backups per criticality; common restore point; immutable or offline copy; access and deletion restricted; restore tested in DR exercises	C	Regular backups	Para 21	16

Control area	Minimum control (target [ML2])	Type	Essential Eight	CPS 234	Policy section
Logging and monitoring (key)	Central, protected logs; timely analysis; incidents reported to CISO; response plan enacted	D	Required within several strategies at ML2	Paras 21, 23	14
Network security	Segmentation, default-deny, minimal attack surface, secure remote access	P	Outside the Essential Eight (ISM)	Para 21	15.1
Endpoint and email	EDR, encryption, email authentication and filtering, web filtering	P/D	Outside the Essential Eight (ISM)	Para 21	15.2–15.3
Encryption and keys	Approved cryptography; key management; cryptographic inventory; post-quantum plan	P	Outside the Essential Eight (ISM)	Para 21	17
Secure development and change	Secure SDLC, code and dependency scanning, change control, pre-release testing	P	Outside the Essential Eight (ISM)	Para 21	18
Third parties and cloud	Capability assessment, design evaluation, contract clauses, ongoing oversight, shared responsibility	P/D	Applies to third-party online services (MFA)	Paras 16, 22, 28, 34	19
Awareness and personnel	Training, phishing simulation, screening	P	Outside the Essential Eight	Para 19	20
Incident response (key)	Response plans and playbooks, tested annually	C	Response plan enacted (ML2)	Paras 23–26	21
Testing and assurance (key)	Systematic testing program by independent specialists; annual sufficiency review; internal audit	D	Essential Eight assessment	Paras 27–34	22–23

CPS 234 paragraph map: roles 13–14 (section 7); capability 15–17 (8); policy framework 18–19 (9); classification 20 (10); controls 21–22 (11–20); incident management 23–26 (21); testing 27–31 (22); internal audit 32–34 (23); APRA notification 35–36 (24).

Appendix B. Information classification scheme

B.1 Sensitivity (confidentiality and integrity)

Label	Description	Examples	Minimum handling
Public	Approved for public release; no harm if disclosed	Published product disclosure statements, website content, annual reports	Integrity protected; publish only through approved channels
Internal	For staff and authorised contractors; limited harm if disclosed	Policies, procedures, internal announcements	Access limited to authenticated staff; no public sharing
Confidential	Disclosure or unauthorised change could cause material harm to customers or [Organisation]	Customer personal information, account data, contracts, non-public financial results, security configurations	Need-to-know access; encryption in transit and at rest; MFA; approved sharing only; logged access
Highly Confidential	Disclosure or unauthorised change could cause severe harm, regulatory action or loss of trust	Large customer data sets, tax file numbers, identity documents, health information, credentials and keys, market-sensitive information, Board papers, incident investigations	Named access, approved by the asset owner; strongest encryption and key control; data loss prevention; enhanced monitoring; no use in test environments; offshore storage only with approval

B.2 Criticality (availability)

Tier	Description	Link to tolerance levels
Tier 1: Critical	Supports a critical operation, or loss would cause severe customer or financial harm within hours	Recovery time and data loss within the critical operation's CPS 230 tolerance levels; tested at least annually
Tier 2: High	Supports important business processes; loss within a day would cause significant harm	Recovery time objective [≤ 24 hours] ; recovery point objective [≤ 4 hours]
Tier 3: Medium	Loss would cause moderate disruption with workarounds	Recovery time objective [≤ 72 hours]
Tier 4: Low	Loss would cause minimal disruption	Best effort

The asset's overall protection level is set by the higher of its sensitivity and criticality. Classification reflects potential financial and non-financial impact on [Organisation] and on depositors, policyholders, beneficiaries and other customers (CPS 234 para 20). Align these impacts with the six impact categories in the RiskFA Risk Management Framework.

Appendix C. Metrics and key risk indicators

Metric / KRI	Typical limit or target
Essential Eight maturity achieved, by strategy, against target	All eight at [ML2] by [date] ; no strategy below [ML1]
Critical or exploited vulnerabilities on internet-facing systems patched within [48 hours]	≥ [95%]
Other vulnerabilities patched within the section 13.3 timeframes	≥ [90%]
Unsupported (end-of-life) systems in production without an approved exception	[0]
Staff accounts protected by phishing-resistant MFA	[100%] of privileged accounts; ≥ [95%] of all staff
Privileged accounts reviewed in the last [quarter] ; dormant privileged accounts disabled	[100%]
Leavers' access removed by last day	≥ [99%]
Endpoints with active EDR and full disk encryption	≥ [98%]
Critical systems sending logs to central monitoring	[100%]
Mean time to detect / contain High and Critical incidents	≤ [x hours] / ≤ [y hours] ; trending down
Backup restoration tests successful and within tolerance (critical operations)	[100%] tested in the last 12 months
Phishing simulation report rate / click rate	Report rate ≥ [60%] ; click rate ≤ [5%]
Security awareness training completed on time	≥ [95%]
Material service providers with a current security assessment	[100%]
Key controls tested in the last cycle; key controls rated ineffective	[100%] tested; ineffective trending down

Metric / KRI	Typical limit or target
Open High and Critical security issues overdue	[0] more than [30 days] overdue
Open exceptions; expired exceptions	Trending down; [0] expired
Penetration test High and Critical findings remediated on time	≥ [95%]
Regulatory notifications (APRA, ASD, OAIC, ASIC) made on time	[100%]

These metrics and limits are common industry practice, not regulatory requirements. Set your own in line with your risk appetite and report them consistently over time.



[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.](#)