

Incident & Issues Management Standard

How to identify, record, rate, escalate, notify, investigate, remediate and close incidents and issues, aligned to current Australian regulation and industry best practice. 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 standard. Adopt the structure, terms and ratings as written, so that your organisation speaks the same language as the rest of the industry. Fill in the text in [square brackets] with your organisation's details, set the thresholds and timeframes to match your size and risk appetite, delete obligations that do not apply to you, and approve the Standard 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	Incident & Issues Management Standard
Organisation	[Organisation name]
Document owner	[Chief Risk Officer]
Approved by	[Board Risk Committee]
Version / date approved	[1.0] / [date]
Review cycle	At least [annually], and after any material change in regulation or the business, or a Critical incident
Parent policy	[Risk Management Framework / Operational Risk Management Policy]

1. Purpose

This Standard sets the minimum requirements for identifying, recording, rating, escalating, notifying, investigating, remediating and closing **incidents** and **issues** across [Organisation]. It ensures that:

- problems are found, recorded and dealt with quickly and consistently;
- the right people, including the Board and regulators, are told within the required timeframes;
- customers who are affected are treated fairly and remediated promptly;
- root causes are fixed, not just symptoms, and fixes are proven to work, so that problems do not recur; and
- management and the Board have accurate, timely information on the organisation's risk and control environment.

The Standard supports [Organisation]'s obligations under its risk management framework, including, where they apply: APRA Prudential Standards CPS 230 *Operational Risk Management*, CPS 234 *Information Security* and CPS 220 / SPS 220 *Risk Management*; the breach reporting (reportable situations) obligations in the *Corporations Act 2001* and *National Consumer Credit Protection Act 2009*; ASIC RG 271 *Internal dispute resolution* and RG 277 *Consumer remediation*; and the *Financial Accountability Regime Act 2023*.

2. Scope

This Standard applies to:

- all employees, contractors, directors and officers of [Organisation] and its subsidiaries;
- all business units, products, services, systems and locations; and
- incidents and issues arising at material service providers and other third parties that affect [Organisation] or its customers. These are recorded and rated in [Organisation]'s register as our own incidents.

Agreements with material service providers must require them to notify [Organisation] of incidents affecting our services, data or customers within [24 hours] (sooner for security incidents), so that we can meet our own notification deadlines.

Specialist processes (for example cyber security incident response, business continuity and crisis management, complaints handling, fraud, privacy, whistleblowing and AML/CTF) may have additional procedures. Those procedures must stay consistent with this Standard, and every incident and issue must still be recorded in the register.

3. Key definitions

Term	Meaning
Event	Anything that happens which has, or could have, an effect on the organisation, its customers or its objectives.
Incident	An event that has caused, or could have caused, a loss, harm, disruption, breach or other adverse outcome. Includes operational risk incidents, breaches, outages, errors, fraud, information security and privacy incidents.
Near miss	An incident that was stopped before it caused an impact. Near misses must be recorded: they show where controls are weak.
Issue	A known gap or weakness in a control, process, system or practice that needs to be fixed, whether or not an incident has happened yet. Issues come from incidents, audits, reviews, risk and control assessments, complaints, regulators or self-identification.
Breach	A failure to comply with a legal, regulatory, licence or contractual obligation, or with an internal policy.
Date identified	The date any employee, contractor or service provider first became aware of facts suggesting a possible incident or issue. Internal timeframes in this Standard run from this date.
Reportable situation	A situation that must be reported to ASIC under Corporations Act s912D or NCCP Act s50A. It includes a significant breach (or likely significant breach) of a core obligation; an investigation into whether one has occurred that continues for more than 60 days (and the outcome of that investigation if it finds no significant breach); conduct constituting gross negligence or serious fraud; and certain conduct of financial advisers or mortgage brokers of other licensees.
Critical operation	A process undertaken by [Organisation] or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on depositors, policyholders, beneficiaries or other customers, or on [Organisation] 's role in the financial system (CPS 230).
Root cause	The underlying reason an incident or issue happened which, if fixed, prevents it from recurring. 'Human error' on its own is never a root cause (see section 12).

Term	Meaning
Extent of condition	Whether the same root cause affects, or could affect, other products, business units, systems, service providers or time periods.
Action	A specific, owned task with a due date that fixes an issue or a root cause.
Customer remediation	Putting affected customers back into the position they would have been in had the incident not happened, including refunds, compensation and interest (RG 277).
Owner	The person accountable for managing an incident, issue or action to closure (see section 6).

4. Principles

1. **Speak up early.** Anyone who sees a possible incident or issue must raise it promptly. Honest mistakes reported promptly are treated as a chance to learn; no one is penalised for raising a genuine concern in good faith.
2. **Record everything.** All incidents (including near misses) and issues are recorded in the register, however small.
3. **Assess honestly.** Ratings reflect the realistic worst impact, not the most convenient one. When in doubt, rate higher and escalate.
4. **Rating never decides reportability.** Every possible breach is assessed for notification, whatever its rating.
5. **Customers first.** Stop the harm, then identify and remediate affected customers fairly and promptly.
6. **Meet the clock.** Regulatory deadlines run from a trigger event (often when the organisation becomes aware), not from when an investigation finishes.
7. **Fix the cause, everywhere.** Significant incidents and issues are investigated to root cause, checked for extent of condition, and fixed at the cause.
8. **Clear ownership.** Every incident, issue and action has one named accountable owner and a due date.
9. **Complete and effective.** Nothing is closed until the fix is complete and shown to work.
10. **Learn.** Themes, repeat incidents and lessons are reported and acted on.

5. Three lines of accountability

Line	Who	Responsibilities
First line	Business units, product and operations owners, technology	Own and manage incidents and issues in their area: identify, record, contain, rate, escalate, investigate, remediate and close them within the required timeframes.
Second line	Risk and Compliance	Own this Standard; provide the register and guidance; review and challenge ratings, root causes, extent of condition and actions; assess breaches and notifications; validate closures; report to management and the Board.
Third line	Internal Audit	Independently assess whether this Standard is designed and operating effectively; raise audit issues, which are managed under this Standard.

6. Roles and responsibilities

Role	Responsibilities
Board	Sets risk appetite; oversees significant incidents, issues, regulatory notifications and customer remediation; holds management to account for fixing root causes on time.
Board Risk Committee	Approves this Standard; receives regular reporting (section 16); is told of Critical incidents within [24 hours] ; approves risk acceptances outside appetite and second extensions of High or Critical actions.
Chief Executive Officer and executive team	Foster a culture of speaking up; ensure incidents and issues in their areas are managed in line with this Standard; own issues in their areas as the accountable executive.
Accountable persons (FAR, where applicable)	Meet their accountability obligations under FAR Act s21, including taking reasonable steps to prevent matters that would adversely affect the entity's prudential standing or reputation, and to prevent material contraventions of the relevant laws, in their areas of responsibility.
Chief Risk Officer	Owns this Standard; ensures independent challenge; approves downgrades of Critical ratings; decides Board escalation of Critical incidents; oversees regulatory notifications with Compliance and Legal.
Head of Compliance / General Counsel	Assess whether a matter is a breach, reportable situation or otherwise notifiable; make or approve notifications to regulators; manage legal privilege where appropriate.
Incident owner	A senior manager in the area where the incident arose. Contains it, ensures it is recorded and rated, leads the investigation, root cause and extent of condition analysis, and coordinates customer remediation.
Issue owner	One accountable executive per issue, even when actions span several areas. Agrees the action plan, monitors progress and provides closure evidence.
Action owner	Completes an assigned action by its due date and provides evidence.
All staff	Identify and report incidents, near misses and issues promptly; cooperate with investigations.

7. The incident lifecycle

Every incident follows these stages. Timeframes are in section 9.

Stage	What must happen
1. Identify	Anyone who becomes aware of a possible incident tells their manager immediately and records it (or ensures it is recorded).
2. Contain	The incident owner acts straight away to stop or limit the impact: stop the process, fix the error, protect customers and data, and invoke business continuity if needed. Critical incidents activate the Crisis Management Team under the RiskFA Crisis Management Plan. Evidence (system logs, records, emails) is preserved from the start and nothing is altered or destroyed.
3. Record	The incident is recorded in the register with the minimum information in Appendix B.
4. Rate	The incident is rated Critical, High, Medium or Low (section 8). Second line reviews the rating.
5. Escalate	The incident is escalated according to its rating (section 9).
6. Assess obligations	Compliance and Legal assess whether it is a breach, reportable situation, notifiable data breach or otherwise notifiable, and whether customers are affected (section 10). This happens for every possible breach, whatever the rating.
7. Communicate	External communications to customers, media and regulators are approved by [CEO / Communications / Legal] .
8. Investigate	The owner establishes the facts, impact, affected customers, root cause and extent of condition (section 12).
9. Remediate	Customers are remediated (section 13). Issues are raised for every control gap, with actions that fix the root cause (section 11).
10. Close	Closed when the impact is resolved, notifications are complete, issues are raised, and customer remediation is complete or tracked as a separate issue until it is. Second line approves closure of High and Critical incidents.
11. Learn	Lessons are shared and trends reported (section 16). Critical incidents have a post-incident review.

8. Rating incidents and issues

Rate on the **highest** rating reached in any one impact category, using the realistic worst-case impact before any expected recoveries. Re-rate as information changes and record the reason.

- **Incidents** are rated on actual or potential impact.
- **Issues** are rated on the likely impact **and** likelihood of harm if the weakness is not fixed, taking account of interim controls.
- **Downgrades:** a rating may be lowered only with second line agreement and a recorded reason. Lowering a Critical rating needs CRO approval.
- **Aggregation:** repeated or similar incidents with a common root cause are linked and rated together on their combined impact. A series of Low incidents can amount to a High issue.

Impact	Critical	High	Medium	Low
Financial (loss, cost or remediation)	≥ [\$5m]	[\$1m] to < [\$5m]	[\$100k] to < [\$1m]	< [\$100k]
Customers	Widespread harm, or serious harm to vulnerable customers	Many customers affected, or significant harm to some	Some customers affected; limited harm	Few or no customers affected; no lasting harm
Regulatory and legal	Significant breach; likely regulator action or licence impact	Breach that is reportable or likely to attract regulator attention	Breach of law or policy with limited consequences	Minor policy breach
Operations and critical operations	Critical operation disrupted beyond tolerance	Critical operation disrupted within tolerance, or major disruption to other operations	Moderate disruption; workarounds in place	Minimal disruption

Impact	Critical	High	Medium	Low
Information security and privacy	Material information security incident (CPS 234) or large-scale eligible data breach	Eligible data breach, or security incident affecting sensitive systems	Contained security or privacy incident; no serious harm likely	Policy breach with no data exposed
Reputation	Sustained national media or public attention; loss of stakeholder confidence	Media or stakeholder attention	Limited external awareness	Internal only

Set the dollar thresholds against your organisation's size, for example Critical at [1%] of annual net profit or [0.5%] of capital. The example values suit a mid-to-large entity; a smaller licensee, fund or insurer might use [\$500k] / [\$100k] / [\$10k] . The CRO can always raise a rating.

9. Escalation and timeframes

Record every incident in the register within [2 business days] of the date identified, and Critical or High incidents the same day.

Step	Critical	High	Medium	Low
Contain	Immediately	Immediately	Promptly	Promptly

Step	Critical	High	Medium	Low
Escalate to	CEO, CRO, General Counsel, relevant executive and accountable person immediately (within [1 hour]); Board Risk Committee chair within [24 hours]	Relevant executive, CRO and Head of Compliance within [24 hours]	Business unit head and second line within [2 business days]	Line manager
APRA materiality decision (CPS 230 / CPS 234)	Within [24 hours] of identification	Within [24 hours] if a critical operation, information asset or customers may be affected	Not usually required	Not usually required
Reportability decision (any possible breach)	Started immediately; decision recorded by day [20]	Decision recorded by day [20]	Decision recorded by day [20]	Decision recorded by day [20]
Root cause and extent of condition	Within [20 business days]	Within [20 business days]	Within [30 business days]	Cause recorded; linked to similar incidents
Post-incident review	Required	At CRO discretion	Not required	Not required

If in doubt, escalate. An incident must never wait for a full investigation before it is escalated or assessed for notification.

10. Regulatory notifications

The rating does not decide whether a matter is reportable. Many low-value breaches are significant under the law. Compliance assesses every incident that may involve a breach of a legal or regulatory obligation, and records the decision and reasons no later than day **[20]** after the date identified, so that any notification can be lodged within the statutory deadline.

For APRA's 72-hour and 24-hour clocks, **[Head of Compliance]** decides within **[24 hours]** of identification whether an incident is likely to have a material financial impact or a material impact on critical operations. As a minimum this covers every Critical incident, and any High incident affecting a critical operation or above **[\$X]**. The decision and reasons are recorded.

All notifications, and decisions not to notify, are recorded with reasons. The table summarises common obligations as at October 2026; delete those that do not apply to you and confirm the current requirements.

Obligation	Applies to	When to notify
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 already notified under CPS 234 need not be notified again.	APRA-regulated entities: ADIs, general, life and private health insurers, RSE licensees and their NOHCs	APRA, as soon as possible and no later than 72 hours after becoming aware
Disruption to a critical operation outside tolerance (CPS 230 para 41): the nature of the disruption, action taken, likely impact and time to return to normal. The Board is also told, with a remediation plan.	APRA-regulated entities	APRA, as soon as possible and no later than 24 hours after suffering the disruption
Information security incident that materially affected, or could have materially affected, the entity or customers, or that has been notified to another regulator in Australia or overseas (CPS 234 para 35)	APRA-regulated entities	APRA, as soon as possible and no later than 72 hours after becoming aware
Material information security control weakness the entity expects it cannot remediate in a timely manner (CPS 234 para 36)	APRA-regulated entities	APRA, no later than 10 business days after becoming aware

Obligation	Applies to	When to notify
Breach of a prudential requirement (Banking Act s62A; Insurance Act s38AA; Life Insurance Act s132A; PHIPS Act s95; SIS Act s29JA)	ADIs, general insurers, life insurers, private health insurers, RSE licensees	APRA. ADIs: immediately if the ADI or its group may not be in a sound financial position; otherwise as soon as practicable and within 10 business days of a significant breach (s62A). General and life insurers: immediately for a breach relating to obligations to policyholders (policy owners) or minimum capital; otherwise as soon as practicable and within 10 business days for other significant breaches or matters materially and adversely affecting financial position (s38AA, s132A). Private health insurers: as soon as practicable (s95). RSE licensees: as soon as practicable and within 30 days (s29JA).
Significant breach of, or material deviation from, the risk management framework, or the framework not adequately addressing a material risk (CPS 220 para 53; SPS 220 para 35)	ADIs, insurers, RSE licensees	APRA, as soon as practicable and no more than 10 business days after becoming aware (CPS 220); within 10 business days (SPS 220) after becoming aware
Reportable situation, including a significant breach of a core obligation, or an investigation continuing for more than 60 days (Corporations Act ss912D, 912DAA; NCCP Act ss50A, 50B; the 60-day period is set by ASIC Instrument 2024/620, see RG 78)	AFS licensees and credit licensees (APRA-regulated licensees may lodge through APRA if the report is complete and on time)	ASIC, within 30 calendar days after first knowing, or being reckless as to whether, there are reasonable grounds to believe a reportable situation has arisen

Obligation	Applies to	When to notify
Reportable situation about a financial adviser or mortgage broker of another licensee (s912DAB; NCCP s50C)	AFS and credit licensees	ASIC, within 30 calendar days
Significant dealing in a product inconsistent with its target market determination (design and distribution obligations, s994G)	Product issuers (distributors notify the issuer)	ASIC, as soon as practicable and within 10 business days of becoming aware
FAR events: an accountable person ceases, is dismissed or suspended, or has variable remuneration reduced for failing their obligations; reasonable grounds to believe the entity or an accountable person breached FAR obligations (FAR Act s31, s32)	Accountable entities under FAR	APRA and ASIC (via APRA Connect), within 30 days
Suspected eligible data breach (Privacy Act Notifiable Data Breaches scheme)	Entities covered by the Privacy Act	Take all reasonable steps to assess within 30 calendar days ; if eligible, notify the OAIC and affected individuals as soon as practicable
Suspicious matter (AML/CTF Act s41)	Reporting entities	AUSTRAC within 24 hours of forming the suspicion for terrorism financing, otherwise within 3 business days (up to 5 business days where legal professional privilege is claimed)
Cyber security incident with a significant (s30BC) or relevant (s30BD) impact on a critical infrastructure asset (SOI Act Part 2B)	Responsible entities for critical banking, superannuation, insurance and financial market infrastructure assets	ASD's Australian Cyber Security Centre within 12 hours (significant) or 72 hours (relevant) of becoming aware; a written report follows within 84 or 48 hours of an oral report

Obligation	Applies to	When to notify
Ransomware or cyber extortion payment (Cyber Security Act 2024 s27)	Businesses with annual turnover above \$3 million (<i>Cyber Security (Ransomware Payment Reporting) Rules 2025</i> s6), 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
Information a reasonable person would expect to have a material effect on price (ASX Listing Rule 3.1)	Listed entities	ASX immediately (promptly and without delay), unless an exception in LR 3.1A applies
Contractual notifications	All	Counterparties, insurers and service providers as the contract requires (check insurance notification terms)

This summary is general information and may not be complete for your organisation. Other notifications (for example APRA notifications about material service provider arrangements under CPS 230 para 60) are covered in other policies. Confirm current requirements with the regulator's guidance or your legal adviser.

11. Issues management

11.1 Raising an issue

An issue must be raised whenever a control gap or weakness is found, from any source: incidents, internal audit, external audit, regulator findings, risk and control self-assessments, compliance monitoring, complaints analysis or self-identification. Each issue is recorded with one accountable owner, a rating (section 8), the root cause and an action plan.

Open issues are linked to the relevant risks and controls in the risk and control assessment, and those controls are rated ineffective or partly effective until the issue is closed. Each open High or Critical issue records the residual risk while it is being fixed, and the interim controls relied on.

11.2 Action plans

Actions must be **specific, owned, achievable and dated**, and together must fix the root cause. Interim controls must be put in place where the full fix will take time.

Issue rating	Action plan agreed	Target completion
Critical	Within [5–10 business days]	Within [3 months]
High	Within [20 business days]	Within [6 months]
Medium	Within [30 business days]	Within [6–9 months]
Low	Within [30 business days]	Within [12 months]

11.3 Due dates, extensions and ownership

- Request an extension **before** the due date, with reasons, progress to date and interim controls.
- Extensions are approved by: Low and Medium, the owner's executive; High, the relevant executive and the CRO; Critical, the CRO, with the Board Risk Committee informed.
- **The original due date is never overwritten.** Reports show both the original and current due dates.
- No action may be extended more than [twice] without Board Risk Committee approval.
- When an owner leaves or changes role, the issue is reassigned within [5 business days].
- Issues raised by regulators or internal audit also follow those parties' agreed processes.

11.4 Risk acceptance

Where [Organisation] decides not to fix an issue, the risk must be formally accepted by a person with the right authority, with reasons and a review date of no more than [12 months]. Acceptances outside risk appetite need Board Risk Committee approval and may be renewed only [once]. Risk acceptance can never be used for a breach of law or for ongoing customer harm.

11.5 Closing an issue: complete and effective

- An issue is closed only when the actions are complete **and** the control has been shown to operate effectively.
- For High and Critical issues, effectiveness is shown by testing over at least **[one control cycle, or 3 months for frequent controls]**, and second line validates the evidence before closure.
- Second line sample-tests at least **[10%]** of Medium and Low closures each **[quarter]**.
- Internal Audit validates closure of internal audit issues; regulator findings are closed in line with the regulator's requirements.
- An issue that recurs, or fails validation, is re-opened under its original ID and original due date, and counted as re-opened in reporting.

12. Investigation and root cause analysis

Investigations establish what happened, when, why, who and what was affected, the full impact, the root cause and the extent of condition. Use a recognised technique such as the **5 Whys** or a **fishbone** (cause and effect) analysis; the quality of the analysis matters more than the technique.

- **'Human error', 'staff error' or 'one-off' is not an acceptable root cause on its own.**
The analysis must explain why the control environment allowed the error and did not detect it, for example process design, system controls, supervision, workload, incentives or culture.
- **Training alone is not an acceptable fix** for a High or Critical matter unless it comes with a control change.
- **Extent of condition:** for every High and Critical incident or issue, the owner checks whether the same root cause could affect other products, business units, systems, service providers or time periods, and records the result. Matters found are raised as linked incidents or issues.
- Second line reviews and challenges root cause analysis for all High and Critical items before it is accepted.

Root cause category	Examples
People	Capacity, supervision, capability, key person dependency (never 'human error' alone)
Process	Missing or unclear procedure, manual workaround, poor design, inadequate checks

Root cause category	Examples
Systems and data	System defect, data quality, access control, capacity
Change management	A failed or poorly controlled change to a product, process, system or organisation
Third parties	Service provider failure, contract gaps, poor oversight
Culture, conduct and incentives	Pressure to meet targets, incentives that reward the wrong outcome, failure to speak up
Governance	Unclear accountability, poor oversight, risk not identified
External events	Natural hazard, cyber attack, external fraud, market event

For Critical incidents, and others at the CRO's discretion, a post-incident review reports the timeline, root causes, extent of condition, the effectiveness of the response and lessons learned to the executive and the Board Risk Committee.

13. Customer remediation

Where customers have suffered, or may have suffered, loss from misconduct or other failures, [Organisation] remediates them fairly, consistently and promptly, in line with ASIC RG 277 *Consumer remediation* where it applies (AFS and credit licensees, including superannuation trustees). In particular:

- start remediation as soon as possible; do not wait until every detail is known before paying customers who are clearly affected;
- start the review period from when [Organisation] reasonably suspects the failure first occurred and caused loss, not from when it was confirmed;
- resolve doubts in favour of the customer, and use beneficial assumptions where records are incomplete;
- include interest or foregone returns for the time value of money, with the methodology documented and approved;
- pay customers proactively, without requiring them to claim, wherever possible, and make reasonable efforts to contact former customers;
- never profit from the failure: amounts that cannot be paid go to the relevant unclaimed money regime or as RG 277 otherwise permits;
- communicate clearly with affected customers and tell them about complaint handling

(internal dispute resolution and AFCA);

- have the methodology reviewed by second line, and consider independent assurance for large programs; and
- track each remediation program as a separate issue, reported to the executive and Board Risk Committee until complete.

14. Complaints, whistleblowing and sensitive matters

- Complaints data is reviewed at least [monthly] for possible incidents and systemic issues, which are recorded in the register and escalated as RG 271 requires.
- A disclosure that may qualify for whistleblower protection is handled under the RiskFA Whistleblower Policy. The register entry must not identify the discloser.
- Access to sensitive records (whistleblower disclosures, staff misconduct, fraud, privacy) is restricted to those who need it.

15. Records and the register

- All incidents, issues and actions are recorded in the [name of GRC system or register], which is the single source of truth.
- Owners keep records accurate, complete and up to date at least [monthly], with every change dated. Original ratings and due dates are kept.
- Supporting evidence (investigations, approvals, notifications, closure evidence) is attached or referenced.
- Records are kept for at least [7 years], or longer where required by law.
- Where Legal directs that an investigation be privileged, follow Legal's instructions on how it is recorded.

16. Reporting, measures and continuous improvement

Second line reports to the executive [monthly] and to the Board Risk Committee [quarterly]. Board reports focus on insight, customer impact and accountability, not volume. Reports cover at least:

- new, open and closed incidents and issues, by rating and business unit;
- Critical and High incidents, regulatory notifications and reportable situations;
- overdue and extended actions, ageing, and original against current due dates;
- operational losses and customer remediation progress;
- repeat incidents, re-opened issues, root cause themes and near misses; and

- performance against the measures below.

Measure	Typical target
Incidents recorded within the required time of identification	$\geq$ [95%]
Average time from occurrence to identification, and from identification to reportability decision	Trending down
Reportable situations and other notifications lodged on time	[100%]
Open actions overdue	$\leq$ [5–10%] ; no High or Critical action more than [90 days] overdue
Actions closed by their original due date	Trending up
Issues re-opened or failing validation	$\leq$ [5%]
Issues found by the business itself (versus audit or regulator)	$\geq$ [70%] ; a falling share is a culture warning sign
Customer remediation programs open more than 12 months	[0]

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

Themes and lessons learned are used to update risk and control assessments, training and procedures.

17. Training and assurance

- All staff complete incident and breach identification training at induction and [annually] , with examples relevant to their role.
- Second line tests register data quality and timeliness at least [half-yearly] .
- Internal Audit reviews the design and effectiveness of this Standard at least every [3 years] .

18. Accountability and compliance with this Standard

Timely, honest identification and reporting of incidents is recognised. Concealment, late reporting, deliberate under-rating and repeatedly overdue actions are breaches of this Standard, are managed under the RiskFA Consequence Management Framework, and are considered in performance and variable remuneration outcomes under the RiskFA Remuneration Policy (CPS 511 where it applies). Exemptions from this Standard need the written approval of the CRO and are reported to the Board Risk Committee.

19. Related documents

- the RiskFA Risk Management Framework, the RiskFA Risk Appetite Statement and the RiskFA Operational Risk Management Policy
- the RiskFA Business Continuity Policy and the RiskFA Crisis Management Plan
- the RiskFA Compliance and Breach Reporting Policy
- the RiskFA Cyber Incident Response Plan and the RiskFA Data Breach Response Plan
- the RiskFA Complaints Handling Policy and the RiskFA Customer Remediation Policy
- the RiskFA Whistleblower Policy, the RiskFA Consequence Management Framework and the RiskFA Remuneration Policy
- APRA: CPS 230 and CPG 230, CPS 234, CPS 220 / SPS 220, CPS 511
- ASIC: RG 78 *Breach reporting by AFS licensees and credit licensees*, RG 271 *Internal dispute resolution*, RG 274 *Product design and distribution obligations*, RG 277 *Consumer remediation*
- OAIC: Notifiable Data Breaches guidance; AUSTRAC: suspicious matter reporting guidance
- Standards: AS ISO 31000 *Risk management*, ISO 22301 *Business continuity*, ISO/IEC 27035 *Information security incident management*, AS ISO 37301 *Compliance management systems*

Appendix A. Rating quick guide

1. Identify every impact category affected (financial, customers, regulatory, operations, information security, reputation).
2. Rate each category using the realistic worst case.
3. The overall rating is the **highest** category rating.
4. Check for similar incidents and rate them together if they share a root cause.
5. If you are unsure between two ratings, choose the higher one and escalate.
6. Remember: the rating does not decide reportability. Send every possible breach to Compliance.

Appendix B. Minimum information to record

Field	Incidents	Issues
Unique ID, title and description	✓	✓
Date occurred, date identified, date recorded	✓	Date identified
Business unit, product, process, system and service provider	✓	✓
How it was identified (source)	✓	✓
Accountable owner	✓	✓
Rating and rationale by impact category; rating history	✓	✓
Loss event type (e.g. Basel categories)	✓	Optional
Customers affected (number, type, vulnerability)	✓	If applicable
Financial impact: gross loss, recoveries, net loss	✓	Estimated
Breach and notification assessment, decision, reasons and dates	✓	If applicable
Root cause, category and extent of condition	✓	✓
Linked risks, controls, incidents and issues	✓	✓
Residual risk and interim controls	If applicable	✓ (High and Critical)
Actions: owner, original and current due date, status, extensions	Linked issues	✓
Closure evidence, validation and approver	✓	✓

Appendix C. Incident report template

Section	Content
1. Summary	What happened, in two or three sentences.
2. Timeline	When it occurred, was identified, was contained; key decisions.
3. Impact	Customers, financial, regulatory, operational, information security, reputation.
4. Rating	Rating and rationale.
5. Immediate response	Containment actions taken; crisis team activation if any.
6. Obligations	Breach and notification assessment; notifications made and when.
7. Root cause	Root cause, category and extent of condition.
8. Remediation	Customer remediation approach and status.
9. Actions	Issues raised, actions, owners and due dates.
10. Lessons learned	What will change as a result.

Appendix D. Closure checklist

- Impact resolved and containment confirmed.
- Rating confirmed and final financial impact recorded.
- Breach and notification assessment completed; notifications made and recorded.
- Root cause and extent of condition recorded, and challenged by second line (High and Critical).
- Affected customers identified; remediation completed or tracked as a separate issue.
- Issues and actions raised for every control gap.
- Fix shown to be effective, and second line validation obtained (High and Critical).
- Lessons learned recorded and shared.

© 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.](#)