

Compliance and Breach Reporting Policy

How an organisation manages its compliance obligations, and identifies, assesses, reports, rectifies and remediates breaches, aligned to the ASIC reportable situations regime, APRA requirements and AS ISO 37301. 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 timeframes to match your size and risk appetite (never longer than the legal deadlines), 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	Compliance and Breach Reporting Policy
Organisation	[Organisation name]
Document owner	[Head of Compliance / General Counsel]
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 in regulation, ASIC or APRA guidance, or the business
Parent framework	the RiskFA Risk Management Framework
Supporting standards	[Incident & Issues Management Standard] , [Compliance Monitoring Procedure] , [Breach Assessment Procedure]

1. Purpose

This Policy sets how [Organisation] manages its compliance obligations and how it identifies, records, assesses, reports, rectifies and remediates breaches. It ensures that:

- every legal, regulatory and licence obligation that applies to the organisation is known, owned and supported by controls;
- compliance with those obligations is monitored and tested, and weaknesses are fixed at the root cause;
- every possible breach is assessed promptly and consistently, and the decision and reasons are recorded;
- reportable situations and other breaches are reported to ASIC, APRA and other regulators within the legal deadlines;
- affected customers are identified and remediated fairly and promptly; and
- the Board and management receive accurate, timely information on compliance and breaches.

The Policy supports [Organisation] 's obligations, where they apply, under the *Corporations Act 2001* (in particular s912A and the reportable situations regime in Pt 7.6 Div 3), the *National Consumer Credit Protection Act 2009* (National Credit Act) s47 and Pt 2-2 Div 5, APRA Prudential Standards CPS 220 / SPS 220 *Risk Management*, CPS 230 *Operational Risk Management* and CPS 234 *Information Security*, the APRA-administered Acts, and the *Financial Accountability Regime Act 2023* (FAR). It follows AS ISO 37301:2023 *Compliance management systems — Requirements with guidance for use*.

2. Scope and application

This Policy applies to all employees, contractors, directors and officers of [Organisation] and its subsidiaries, to authorised representatives and credit representatives, and to material service providers who perform activities on our behalf. [Organisation] must report reportable situations that involve its representatives as well as its own conduct (s912D(1); s50A(1); RG 78.28).

Main compliance and breach reporting requirements (as at October 2026)	
If [Organisation] is	
An AFS licensee (including a responsible entity, trustee company or RSE licensee)	Corporations Act s912A general obligations; reportable situations to ASIC (s912D, s912DAA, s912DAB); notify, investigate and remediate obligations for personal advice to retail clients (s912EA, s912EB); ASIC RG 78 and RG 104.

If [Organisation] is	Main compliance and breach reporting requirements (as at October 2026)
A credit licensee	National Credit Act s47 general obligations, including adequate compliance arrangements and a written plan documenting them; reportable situations to ASIC (s50A, s50B, s50C); notify, investigate and remediate obligations for mortgage brokers (s51A, s51B); ASIC RG 78 and RG 205.
An ADI, general insurer, life company or private health insurer	CPS 220 (compliance function para 43; prudential compliance mechanisms para 35(f); notification para 53); breach notification to APRA under Banking Act s62A, Insurance Act s38AA, Life Insurance Act s132A or PHIPS Act s95; CPS 230 and CPS 234 notifications; FAR.
An RSE licensee (superannuation trustee)	SPS 220 (prudential compliance mechanisms para 22(b)(iv); notification para 35); SIS Act s29JA breach reporting to APRA; CPS 230 and CPS 234; FAR; and, as an AFS licensee, the ASIC reportable situations regime.
A product issuer or distributor	Design and distribution obligations, including notifying ASIC of significant dealings (s994G) and ASIC RG 274.
A reporting entity under the AML/CTF Act 2006	AUSTRAC reporting, including suspicious matter reports (s41), and the tipping-off prohibition (s123).

CPS 220 does not apply to RSE licensees: they apply SPS 220. SPS 220 does not contain an equivalent of the CPS 220 para 43 'designated compliance function' requirement, but RSE licensees must still have mechanisms for monitoring and ensuring ongoing compliance with all prudential requirements (SPS 220 para 22(b)(iv)). An independent compliance function is good practice for every organisation.

3. Key definitions

Incident, Issue, Breach, Root cause, Extent of condition, Action, Customer remediation and Date identified have the meanings in the RiskFA Incident & Issues Management Standard.

Term	Meaning
------	---------

Term	Meaning
Compliance obligation	A requirement [Organisation] must comply with (law, regulation, licence condition, prudential standard, enforceable regulatory guidance such as the enforceable paragraphs of RG 271, court order or enforceable undertaking), or one it chooses to comply with (industry code, contract, internal policy) (AS ISO 37301).
Compliance risk	The likelihood and consequences of failing to comply with a compliance obligation.
Obligations register	The single record of [Organisation] 's compliance obligations, each mapped to an owner, the processes and controls that meet it, and its monitoring (section 9 and Appendix C).
Compliance plan	A documented, risk-based plan of the compliance activities (monitoring, testing, training, reviews) for a period. Separately, a registered managed investment scheme must have a compliance plan under Corporations Act Ch 5C (s601HA).
Possible breach	Any matter that may involve a failure to comply with a compliance obligation, before it has been assessed. Every possible breach is assessed under this Policy.
Core obligation	The obligations defined in Corporations Act s912D(3) (AFS licensees) and National Credit Act s50A(3) (credit licensees), summarised in RG 78 Appendix 1. They include the general licensee obligations (s912A, s912B; s47) and compliance with specified financial services laws or credit legislation.
Significant breach	A breach of a core obligation that is a deemed significant breach (s912D(4); s50A(4)), or is significant having regard to the factors in s912D(5) / s50A(5) (section 13).
Likely breach	A situation where [Organisation] or its representative is no longer able to comply with a core obligation and the breach, if it occurs, will be significant (s912D(1)(b); s50A(1)(b); RG 78.21).
Reportable situation	A matter that must be reported to ASIC under s912D / s50A, as described in section 14 and the RiskFA Incident & Issues Management Standard.
Reportable investigation	An investigation into whether there is a significant breach or likely significant breach of a core obligation that continues for more than 60 days (s912D(1) (c) / s50A(1)(c) as modified by s6A of ASIC Instrument 2024/620).

Term	Meaning
Reasonable grounds to believe	Facts or evidence that would induce, in a reasonable person, a belief that a reportable situation has arisen. It is an objective test and does not require certain proof (RG 78.85–RG 78.87).
Date of knowledge	The date [Organisation] first knows that, or is reckless with respect to whether, there are reasonable grounds to believe a reportable situation has arisen. ASIC's 30-day period runs from this date (s912DAA(3); s50B(4)).
Rectification	Stopping the breach and fixing the cause so that it does not recur.
Affected client	For the notify, investigate and remediate obligations: a retail client who received personal advice on a relevant financial product, or a consumer who received mortgage broking credit assistance (s912EA; s51A; INFO 259).

4. Principles

1. **Know our obligations.** Every applicable obligation is in the obligations register, with an owner and controls.
2. **Compliance is owned by the business.** The first line meets the obligations; Compliance sets the framework, advises, monitors and challenges.
3. **Speak up early.** Anyone who sees a possible breach raises it straight away. No one is penalised for raising a genuine concern in good faith.
4. **Assess every possible breach.** The incident rating never decides reportability. Small dollar breaches can be significant.
5. **Meet the clock.** Legal deadlines run from when anyone in the organisation knows the facts, not from when a committee, the Board or a lawyer signs off (RG 78.92–RG 78.98).
6. **Report when the grounds exist.** Do not wait for an investigation to finish, legal advice, Board consideration or rectification if that would take us past the deadline (RG 78.60, RG 78.98).
7. **Fix and remediate.** Stop the breach, fix the root cause and remediate affected customers fairly and promptly.
8. **Record the reasons.** Every assessment, decision to report and decision not to report is recorded with its reasons.

5. Three lines of accountability

Line	Who	Responsibilities
First line	Business units, product, operations and technology owners	Own and meet the compliance obligations in their area; design and operate controls; complete compliance attestations; identify, record and escalate possible breaches; contain and rectify breaches; remediate customers.
Second line	Compliance (and Risk)	Own this Policy, the obligations register and the compliance plan; advise on obligations; monitor and test compliance; assess possible breaches and decide reportability; lodge reports with regulators; challenge rectification and remediation; report to management and the Board.
Third line	Internal Audit	Independently assess whether this Policy and the compliance management system are designed and operating effectively, including the timeliness and quality of breach assessments and reports.

6. Roles and responsibilities

Role	Responsibilities
Board	Approves this Policy; sets the tone for a culture of compliance and transparent breach reporting; oversees significant breaches, reportable situations, regulatory notifications and remediation; holds management to account for fixing root causes.
Board Risk Committee	Recommends this Policy to the Board; receives compliance and breach reporting (section 21); oversees the compliance plan, the adequacy of compliance resources and the independence of the compliance function.
Chief Executive Officer and executive team	Ensure their areas meet their compliance obligations; make sure possible breaches are escalated without delay; provide resources for rectification and remediation.
Accountable persons (FAR, where applicable)	Take reasonable steps, in their areas of responsibility, to prevent matters that would adversely affect the entity's prudential standing or reputation and to prevent material contraventions of the relevant laws (FAR Act s21).
Head of Compliance / General Counsel	Leads the compliance function; owns the obligations register, compliance plan and breach register; decides whether a matter is a breach, significant and reportable; approves and lodges reports to ASIC and APRA; has direct, unfettered access to the CEO, the Board Risk Committee and its chair.
Chief Risk Officer	Ensures compliance risk is managed within risk appetite and integrated with the risk management framework; is consulted on Critical and High breaches.
Obligation owner	A named senior manager accountable for meeting a compliance obligation: keeps the register entry current, makes sure controls work, completes attestations and reports possible breaches.
Incident owner and Issue owner	As defined in the RiskFA Incident & Issues Management Standard. Contain, investigate, rectify and remediate breaches in their area.
All staff and representatives	Know the obligations that apply to their role; follow policies and controls; report possible breaches immediately; cooperate with investigations.

7. Regulatory and standards framework

Source	What it requires or provides
Corporations Act Pt 7.6 Div 3 Subdiv B (s912D, s912DAA, s912DAB, s912DAD)	Reportable situations: what must be reported, the 30-day deadline, reports about other licensees' advisers, and ASIC publication of breach data.
Corporations Act Pt 7.6 Div 3 Subdiv C (s912EA, s912EB)	Notify, investigate and remediate affected clients for reportable situations involving personal advice to retail clients.
National Credit Act Pt 2-2 Div 5 (s50A, s50B, s50C, s51A, s51B)	Equivalent obligations for credit licensees, including mortgage brokers.
ASIC Instrument 2024/620 (as amended by Instrument 2025/289)	Single breaches of RG 271 enforceable paragraphs not deemed significant (s5); certain minor breaches not deemed significant (s6); 60-day investigation trigger (s6A); 90 days for further similar reportable situations (s7); content of reports lodged with APRA (s7A).
ASIC RG 78 (updated 21 October 2026)	ASIC's guidance on breach reporting, including significance, investigations, timing, grouping, compliance systems and breach registers.
ASIC INFO 259	Guidance on the notify, investigate and remediate obligations.
APRA CPS 220 / SPS 220	Compliance function (CPS 220 para 43); mechanisms to monitor and ensure compliance with prudential requirements (CPS 220 para 35(f); SPS 220 para 22(b)(iv)); notification of significant breaches of the risk management framework (CPS 220 para 53; SPS 220 para 35).
APRA-administered Acts	Breach notification to APRA: Banking Act s62A, Insurance Act s38AA, Life Insurance Act s132A, PHIPS Act s95, SIS Act s29JA.
AS ISO 37301:2023	International requirements for a compliance management system: compliance obligations, compliance risk assessment, compliance function, culture, monitoring, raising concerns, investigation, nonconformity and corrective action, and continual improvement.

8. The compliance function

[Organisation] has a designated compliance function, led by the [Head of Compliance], that assists senior management to manage compliance risk effectively. For ADIs and insurers this is required by CPS 220 para 43: the function must be adequately staffed by appropriately trained and competent persons who have sufficient authority to perform their role effectively, and have a reporting line independent from business lines. [Organisation] applies the same standard across the group.

- The [Head of Compliance] reports to [the CEO / General Counsel / CRO] and has direct and unfettered access to the [Board Risk Committee] and its chair, and meets the chair without management present at least [annually].
- The compliance function has no revenue-generating responsibilities, and its remuneration is not linked to the performance of the business lines it oversees.
- The function has access to all records, systems, staff and service providers it needs.
- The adequacy of compliance resources is reviewed at least [annually] and reported to the [Board Risk Committee]. Backlogs that delay breach assessment are escalated: ASIC treats unexplained delays as a sign of inadequate compliance arrangements and possible recklessness (RG 78.57, RG 78.91, RG 78.137).
- Compliance staff are trained on the obligations they oversee and on RG 78 at least [annually].

9. Obligations register

The obligations register is the single source of truth for [Organisation]'s compliance obligations. It is kept in [GRC system] and contains, as a minimum, the fields in Appendix C.

- Every obligation has one named **obligation owner** and is mapped to the processes, key controls and policies that meet it, and to the risks in the risk and control assessment.
- Each obligation is rated for compliance risk using the RiskFA rating scale (Critical, High, Medium, Low), taking into account the consequences of non-compliance (including whether it is a core obligation, a civil penalty provision or an offence) and the effectiveness of controls.
- Compliance monitors regulatory change (new and amended laws, prudential standards, ASIC and APRA instruments and guidance, codes and AFCA approaches). Each change is assessed, the register is updated, and implementation is tracked as an action with an owner and due date, before the change takes effect.
- Obligation owners confirm at least [annually] (and [quarterly] for Critical and High obligations) that their entries are complete and accurate and that the controls are

operating.

- Licence conditions, enforceable undertakings, court orders and regulator commitments are recorded as obligations with a due date and an accountable executive.

10. Compliance risk assessment and the compliance plan

Compliance assesses compliance risk across the obligations register at least [annually], using incidents, breaches, complaints, audit findings, regulator feedback and regulatory change. The results drive a risk-based **compliance plan**, approved by the [Board Risk Committee] each [financial year], that sets out:

- the monitoring and testing program, focused on Critical and High compliance risks and core obligations;
- compliance training and awareness activities;
- planned reviews (for example product reviews, conflicts of interest, representative supervision, IDR compliance audits under RG 271.189–RG 271.190);
- regulatory change implementation; and
- the resources needed, and any gaps.

Where the law requires a specific compliance document it is maintained as part of this framework, for example a compliance plan for each registered managed investment scheme (Corporations Act s601HA) and, for credit licensees, a written plan documenting the arrangements and systems that ensure compliance with s47 obligations (RG 78.149). Progress against the compliance plan is reported to the [Board Risk Committee] [quarterly].

11. Compliance monitoring and testing

Compliance monitoring and testing gives the Board evidence that obligations are being met. It covers both control design and operating effectiveness, consistent with the RiskFA Risk Management Framework.

Activity	Who	Frequency
Control self-assessment and compliance attestation	Obligation and control owners (first line)	[Quarterly] for Critical and High obligations; [annually] for others
First line quality assurance (for example file reviews, call monitoring, claims and complaints QA)	First line	Ongoing, per procedure

Activity	Who	Frequency
Compliance monitoring reviews and control testing	Compliance (second line)	Per the compliance plan
Thematic and product reviews	Compliance (second line)	Per the compliance plan
Data analytics and key risk indicators (for example complaints, exceptions, overrides)	First and second line	[Monthly]
Independent assurance	Internal Audit (third line)	Per the internal audit plan

- Findings are rated and recorded as issues under the RiskFA Incident & Issues Management Standard, with an owner, root cause and due date.
- Any finding that may be a breach is immediately sent for breach assessment (section 13). A routine review that finds a possible breach and moves into a targeted inquiry may start a reportable investigation (RG 78.55(c), Example 6(a)).
- Repeated minor breaches of the same kind are analysed together: they may show that compliance arrangements are inadequate (s912D(5)(a) and (c)).

12. Identifying and escalating possible breaches

- Anyone who becomes aware of a possible breach must tell their manager and **[Compliance]** **immediately**, and in any case within **[1 business day]**, and record it (or ensure it is recorded) under the RiskFA Incident & Issues Management Standard.
- Possible breaches come from any source: staff, controls and exceptions, monitoring and audits, complaints, whistleblower disclosures, service providers, representatives, regulators and AFCA.
- Record the **date identified** and, separately, the **date of knowledge** (section 3). For a body corporate, the knowledge of a director, employee or agent acting within the scope of their actual or apparent authority is attributed to the licensee (s769B; National Credit Act s324). ASIC's clock can start when a compliance officer first has the facts, not when a committee or the CEO approves the report (RG 78.92–RG 78.97, Case study 4).
- Compliance must be told of every matter that may involve a breach of a legal or regulatory obligation, whatever its incident rating.
- Representatives and material service providers must report possible breaches to **[Organisation]** within **[2 business days]** (immediately for serious matters), under their agreements (RG 78.136).

13. Assessing breaches

Compliance assesses every possible breach, and records the decision and reasons no later than **day [20]** after the date identified, so that any report can be lodged within the legal deadline. The worksheet in Appendix A and the decision table in Appendix B are used. Where the facts are clear, the assessment and report must be done sooner.

13.1 Steps in the assessment

1. **Is there a breach or likely breach?** Identify the facts, the obligation and whether it has been, or will be, breached. Where facts are still being gathered, start an investigation and track its start date (section 15).
2. **Is it a core obligation?** Check RG 78 Appendix 1 and the obligations register. Breaches of other obligations are still recorded, rectified and assessed for other notifications.
3. **Is it an additional reportable situation?** Gross negligence or serious fraud must be reported regardless of significance (s912D(2); s50A(2); RG 78.63).
4. **Is it a deemed significant breach?** Check the deeming categories in s912D(4) / s50A(4) (RG 78.35), then any exclusion in the regulations or ASIC Instrument 2024/620 (sections 13.2 and 13.3).
5. **If not deemed significant, is it significant?** Consider all the factors in s912D(5) / s50A(5) (section 13.4).
6. **Is another report or notification required?** For example to APRA, under the notify, investigate and remediate obligations, DDO, FAR, OAIC or AUSTRAC (sections 16 to 18).
7. **Are customers affected?** Identify affected customers and start remediation planning (section 19).
8. **Record the decision.** Record the conclusion, reasons, the date of knowledge, the reporting deadline and the approver.

13.2 Deemed significant breaches

A breach or likely breach of a core obligation is taken to be significant if it (s912D(4); s50A(4); RG 78.35):

- is an offence punishable by imprisonment of 3 months or more if it involves dishonesty, or 12 months or more in any other case;
- is a contravention of a civil penalty provision, unless excluded by the regulations (Corporations Regulations reg 7.6.02A(2); National Credit Regulations reg 12A) or ASIC Instrument 2024/620;
- for credit licensees, is a contravention of a key requirement under s111 of the National Credit Code, unless excluded (National Credit Regulations reg 12B);
- is a contravention of the misleading or deceptive conduct provisions (Corporations Act s1041H(1); ASIC Act s12DA(1)); or
- results, or is likely to result, in **material loss or damage** to clients (or, for a managed investment scheme or superannuation entity, to members). Loss or damage includes non-financial loss; consider the affected person's circumstances and aggregate the loss

across all affected people (RG 78.42–RG 78.44).

13.3 Breaches excluded from deeming (ASIC Instrument 2024/620)

- A **single** breach of an enforceable paragraph of RG 271 is not deemed significant only because it is a civil penalty provision (s5; RG 78.37(c)). Multiple or systemic IDR breaches may still be significant (RG 78 Example 4(d)).
- A misleading or deceptive conduct (or false or misleading representation) breach is not deemed significant if it gives rise to only a single reportable situation, impacts only one person (or joint holders), and has not caused and is unlikely to cause any financial loss (s6; RG 78.38(a)).
- Since 27 June 2025, a breach of a core obligation that would only be deemed significant because it is a civil penalty provision or misleading conduct is also not deemed significant if **all** of these apply: it gives rise to a single reportable situation (or a single group of the same or substantially similar conduct within 60 days); for AFS licensees, it is not a contravention of s828C or s981M; no more than **10** persons are impacted; total financial loss is no more than **\$1,000** (whether or not remediated); and it is rectified, including remediation, within **60 days** after it first occurred (s6 as amended by Instrument 2025/289; RG 78.38(b)).
- If further breaches or losses later emerge so that the conditions are no longer met, the matter must be reported (RG 78.39).
- An excluded breach must still be checked against the other deeming categories (for example offences and material loss) and the significance factors (RG 78.40–RG 78.41). Excluded breaches are still recorded in the breach register.

13.4 Significance factors

For a breach of a core obligation that is not deemed significant, Compliance considers **all** of the following, and a breach may be significant on one factor alone (s912D(5); s50A(5); RG 78.45–RG 78.47):

Factor	Questions to ask
The number or frequency of similar breaches (s912D(5)(a))	Has this happened before? Check the breach register. Repeated minor breaches may show an underlying systemic problem or an inability to comply.
The impact on the ability to supply the financial services or credit activities covered by the licence (s912D(5)(b))	Does it affect financial requirements, key persons, resources, systems or service providers needed to provide the licensed services?

Factor	Questions to ask
The extent to which it indicates that compliance arrangements are inadequate (s912D(5)(c))	How long did it go undetected? Did our controls find it? How long did it take to investigate and assess? Is it isolated or broader?
Any other matters prescribed by the regulations (s912D(5)(d))	Check the current regulations.

ASIC considers that a failure to report a significant breach is likely, in itself, to be a significant breach, because it indicates that compliance arrangements may be inadequate (RG 78.133).

14. Reporting reportable situations to ASIC

14.1 What must be reported

Type of reportable situation	Law	Significance test?
Significant breach of a core obligation	s912D(1)(a); s50A(1)(a)	Yes: deemed, or the s912D(5) / s50A(5) factors
Likely significant breach of a core obligation	s912D(1)(b); s50A(1)(b)	Yes
Investigation into whether there is a significant breach or likely significant breach that continues for more than 60 days	s912D(1)(c); s50A(1)(c), as modified by s6A of Instrument 2024/620	No determination of significance needed before reporting
The outcome of such an investigation if it finds no significant breach or likely breach	s912D(1)(d); s50A(1)(d)	Not applicable
Conduct constituting gross negligence, or serious fraud, in providing financial services or credit activities	s912D(2); s50A(2)	No
Reportable situation about an individual financial adviser or mortgage broker of another licensee (other than a reportable investigation)	s912DAB; s50C	As for the underlying reportable situation

14.2 When to report

- Lodge the report within **30 calendar days** after [Organisation] first knows that, or is reckless with respect to whether, there are reasonable grounds to believe the reportable situation has arisen (s912DAA(3); s50B(4); RG 78.83).
- Where a reportable situation has already been reported, a further reportable situation with the same or substantially similar underlying circumstances may be reported within **90 days** (s7 of Instrument 2024/620; RG 78.84). ASIC may direct a shorter period. The grouping test (similar, related or identical conduct **and** the same root cause) applies (RG 78.110–RG 78.115).
- An investigation becomes a reportable situation on **day 61**, and the report is due within 30 days of that date. The outcome, if it finds no reportable situation, must also be reported within 30 days of that finding (RG 78.102, RG 78.105, Example 11).
- If reasonable grounds to believe a reportable situation has arisen exist before an investigation finishes, report it then; do not wait for the investigation to end (RG 78.60, RG 78.106).
- Do not delay beyond the deadline for Board consideration, legal advice, rectification, or (for a likely breach) the breach actually occurring (RG 78.98–RG 78.99).
- For a report about another licensee's adviser or mortgage broker, also give a copy of the report to the other licensee within the same 30 days (s912DAB(5); s50C(5); RG 78.74). No report (and so no copy) is needed only if there are reasonable grounds to believe ASIC already knows of the reportable situation and has all the required information, which ASIC describes as a high threshold (s912DAB(4); s50C(4); RG 78.80).

14.3 How to report

- Reports are lodged in the prescribed form (the approved form for credit licensees) through the ASIC Regulatory Portal (s912DAA(2); s50B(3); RG 78.107). Table 8 of RG 78 lists the content; the breach register holds the same information (RG 78.145).
- Reports are approved by the [Head of Compliance] (or delegate). Critical matters are also notified to the [CEO] and [Board Risk Committee chair] before or at lodgement, but lodgement is never delayed for that purpose.
- Further reportable situations from the same root cause, rectification progress and completion of remediation are notified using the Portal update function while the original report remains open (RG 78.115–RG 78.116).
- An APRA-regulated licensee may meet the ASIC obligation by lodging a report with APRA within the same timeframe, provided the report contains all the information required by s7A of Instrument 2024/620 (s912DAA(5); s50B(6); RG 78.109).
[Organisation] [does / does not] use this option.
- Related entities with the same root cause may be listed in one report (RG 78.114).

14.4 Consequences of not reporting

Failing to report a reportable situation can attract civil penalties and is a criminal offence (other than for reports about other licensees) (RG 78.123–RG 78.126). ASIC must publish information about reportable situations each financial year, within four months after the end of the financial year (s912DAD; s50D; RG 78.127).

15. Investigations

- An investigation starts, as a matter of fact, when [Organisation] begins a searching inquiry to find out whether a significant breach has occurred, for example by gathering information from staff, clients or experts. It does not depend on what the activity is called, or which team does it (RG 78.50–RG 78.56, RG 78.104, Example 10). Merely logging an incident, or short preliminary fact-finding in response to a complaint, is not usually an investigation (RG 78.51(a), RG 78.55).
- The investigation start date is recorded in the breach register, and the register flags investigations at day [30], day [45] and day [55], so that a report can be prepared if the investigation will pass 60 days.
- Investigations are started without unreasonable delay and resourced to finish promptly. Investigations open for more than [60 days] are reviewed [monthly] by the [Head of Compliance], covering progress, reasons for delay, next steps and the significance of the breach (RG 78.57–RG 78.59, RG 78 Table 10).
- Two inquiries into the same subject matter are treated as one investigation from the start of the first (RG 78 Case study 2).
- Do not wait for an investigation to finish before fixing a known deficiency or limiting harm (RG 78.58).
- Where Legal directs that an investigation be privileged, follow Legal's instructions on how it is recorded. Privilege does not change reporting deadlines.

16. Notify, investigate and remediate obligations (personal advice and mortgage broking)

These obligations apply where all four of these circumstances exist: personal advice to a retail client on a relevant financial product (or mortgage broking credit assistance for a credit contract secured by a mortgage over residential property); reasonable grounds to believe a significant breach of a core obligation, gross negligence or serious fraud has arisen; reasonable grounds to suspect the client has suffered or will suffer loss or damage as a result; and reasonable grounds to suspect the client has a legally enforceable right to recover that loss from [Organisation] (s912EA, s912EB; National Credit Act s51A, s51B; INFO 259).

Action	What must be done	Timeframe
--------	-------------------	-----------

Action	What must be done	Timeframe
1. Notify affected clients	Take reasonable steps to notify affected clients in writing of the reportable situation, in ASIC's approved form if one has been approved (s912EA(2); s51A(2)). Good practice: also explain how to complain, including to AFCA	Within 30 days after [Organisation] first knows, or is reckless as to whether, the circumstances exist
2. Investigate	Start an investigation into the nature and full extent of the reportable situation, identify the conduct and quantify the loss; complete it as soon as reasonably practicable	Start within 30 days
3. Notify the outcome	Take reasonable steps to notify each affected client in writing of the outcome, including those found not to have suffered recoverable loss	Within 10 days of the investigation concluding
4. Remediate	Take reasonable steps to pay affected clients an amount equal to the loss or damage	Within 30 days of the investigation concluding

Records must be kept to show compliance with these obligations. Clients outside the scope of these obligations are still considered for remediation under the RiskFA Customer Remediation Policy and RG 277.

17. Notifications to APRA

APRA-regulated entities assess every possible breach of a prudential requirement and every significant breach of the risk management framework for notification to APRA, in parallel with the ASIC assessment.

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

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
Operational risk incidents, critical operation disruptions and information security incidents (CPS 230 paras 32 and 41; CPS 234 paras 35 and 36)	APRA-regulated entities	As set out in section 10 of the RiskFA Incident & Issues Management Standard

APRA breach notifications are lodged through APRA Connect. In assessing significance for APRA, consider the number or frequency of similar breaches, the impact on the ability to conduct business, whether the breach indicates that compliance arrangements may be inadequate, and the actual or potential financial loss to depositors, policyholders or members.

18. Other notifications

The RiskFA Incident & Issues Management Standard section 10 is the master table of regulatory notifications. The obligations most often triggered by breaches are:

Obligation	Applies to	When to notify
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, including 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
Suspicious matter (AML/CTF Act s41). Do not disclose an SMR except as the law permits (s123); a report to ASIC under s912DAB does not breach s123 (RG 78.78–RG 78.79)	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)
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 (see the RiskFA Data Breach Response Plan)
Industry code breaches	Code subscribers	As the relevant code and its compliance committee require
Contractual notifications	All	Counterparties, insurers (including professional indemnity insurers) and service providers as the contract requires

19. Rectification, remediation and preventing recurrence

- Every breach is contained and rectified, and its root cause and extent of condition are analysed under the RiskFA Incident & Issues Management Standard (sections 11 and 12). Issues are raised for every control gap.
- Affected customers are identified and remediated fairly, consistently and promptly under the RiskFA Customer Remediation Policy and ASIC RG 277 *Consumer remediation*. Remediation is not delayed for commercial reasons (RG 78 Example 3(g)).
- The report to ASIC records rectification and remediation plans and dates, and ASIC is updated when they are complete (RG 78 Table 8).
- Lessons learned are used to update the obligations register, controls, training and procedures.
- Consequence management is considered for significant breaches, including for those responsible for oversight (RG 78 Table 10), under the RiskFA Consequence Management Framework.

20. Breach register and records

- All possible breaches, breaches and reportable situations are recorded in the breach register within the [GRC system], linked to the incident and issue records. ASIC expects licensees to keep a breach register that contains the information in the prescribed reporting form (RG 78.144–RG 78.145).
- The register records at least: the facts; the obligation; the date the breach occurred, date identified and date of knowledge; any investigation start and end dates; the assessment against each deeming category, exclusion and significance factor, with reasons; the decision, decision-maker and date; reporting deadlines and the dates reports and updates were lodged, with reference numbers; customers affected and remediation; rectification and root cause; and related breaches.
- Decisions **not** to report are recorded with the same care as decisions to report.
- Records are kept for at least [7 years], or longer where the law requires.
- Compliance tests breach register data quality and timeliness at least [half-yearly].

21. Board and management reporting

Compliance reports to the [Executive Risk Committee] [monthly] and to the [Board Risk Committee] [quarterly]. Reports focus on insight, customer impact and accountability. They cover at least:

- reportable situations and other regulatory notifications lodged in the period, and any

lodged late, with reasons;

- significant breaches, their root causes, rectification and remediation status;
- open investigations, their age, and any approaching the 60-day trigger;
- breach themes, repeat breaches and what they say about compliance arrangements;
- progress against the compliance plan and the results of monitoring and testing;
- regulatory change and its implementation status;
- regulator engagement, findings and commitments; and
- the adequacy of compliance resources.

The Board is told of Critical breaches and of any matter with potential licence, enforcement or significant reputation consequences within [24 hours] through the [Board Risk Committee chair]. The Board is informed of, but does not approve, reports to regulators.

22. Measures and key risk indicators

Measure	Typical target
Reportable situations and other notifications lodged on time	[100%]
Breach assessments recorded by day [20] after the date identified	≥ [95%]
Average days from occurrence to identification, and from identification to decision	Trending down
Investigations open more than 60 days	Each reported to ASIC; number trending down
Breaches found by the business itself (rather than audit, regulators or complaints)	≥ [70%]
Repeat breaches with the same root cause	Trending down
Compliance plan activities completed on schedule	≥ [90%]
Obligation owner attestations completed on time	≥ [95%]
Regulatory changes implemented by their effective date	[100%]

These targets are common industry practice, not regulatory requirements. A higher number of reports can reflect stronger detection rather than worse compliance (RG 78.131). Set your own targets in line with your risk appetite.

23. Training, culture and assurance

- All staff and representatives complete compliance and breach identification training at induction and **[annually]**, with examples relevant to their role. People who assess breaches are trained on RG 78 and Instrument 2024/620.
- Senior management champion transparent reporting, prioritise investigations, rectification and remediation, and make clear who is accountable end to end for breach reporting (RG 78.140–RG 78.141).
- Concealing a breach, delaying escalation or discouraging reporting is a breach of this Policy and is managed under the RiskFA Consequence Management Framework. Concerns may also be raised under the RiskFA Whistleblower Policy.
- Compliance reviews the breach reporting process **[annually]**, including the number of incidents assessed and outcomes, trends and timeliness (RG 78 Table 10).
- Internal Audit reviews this Policy and the compliance management system at least every **[3 years]**.

24. Related documents

- the RiskFA Risk Management Framework, the RiskFA Risk Appetite Statement and **[Incident & Issues Management Standard]**
- the RiskFA Complaints Handling Policy and the RiskFA Customer Remediation Policy
- the RiskFA Data Breach Response Plan and the RiskFA Cyber Incident Response Plan
- **[Conflicts of Interest Policy]**, the RiskFA Whistleblower Policy, the RiskFA Consequence Management Framework and **[FAR Accountability Map]**
- ASIC: RG 78 *Breach reporting by AFS licensees and credit licensees*, INFO 259, RG 104 *AFS licensing: Meeting the general obligations*, RG 205 *Credit licensing: General conduct obligations*, RG 271 *Internal dispute resolution*, RG 274 *Product design and distribution obligations*, RG 277 *Consumer remediation*
- APRA: CPS 220 / SPS 220, CPS 230, CPS 234, CPS 510 / SPS 510
- Standards: AS ISO 37301:2023 *Compliance management systems*, AS ISO 31000:2018 *Risk management — Guidelines*

Appendix A. Breach assessment worksheet

Question	Record
1. Reference, title and short description of the facts	
2. Date occurred (first and last), date identified, date of knowledge, investigation start date (if any)	
3. Obligation(s) involved, with section, licence condition or paragraph	
4. Is there a breach, or a likely breach (no longer able to comply)? Reasons	Yes / No / Still investigating
5. Is it a core obligation (RG 78 Appendix 1)?	Yes / No
6. Is it gross negligence or serious fraud?	Yes / No. If yes, reportable
7. Deemed significant? Offence (3 months dishonesty / 12 months other); civil penalty provision; National Credit Code key requirement; misleading or deceptive conduct; material loss or damage	Category and reasons
8. Does an exclusion apply? (regulations; Instrument 2024/620 s5 single RG 271 breach; s6 single person no loss; s6 ≤ 10 persons, ≤ \$1,000, rectified within 60 days)	Which, with evidence that every condition is met
9. If not deemed: significance factors (number or frequency of similar breaches; impact on ability to provide licensed services; inadequacy of compliance arrangements; prescribed matters)	Assessment of each factor
10. Has an investigation passed, or will it pass, 60 days?	Day 61 date and report due date
11. Conclusion: reportable situation? Type	Yes / No
12. ASIC report due date (30 days, or 90 days for a further similar situation) and lodgement reference	
13. Copy to another licensee required (s912DAB / s50C)?	Yes / No
14. Notify, investigate and remediate obligations triggered? Dates for each action	Yes / No

Question	Record
15. APRA notification (prudential breach, CPS 220 / SPS 220, CPS 230 / CPS 234)? Due date	Yes / No
16. Other notifications (DDO, FAR, AUSTRAC, OAIC, code, insurer)?	List
17. Customers affected, estimated loss, remediation approach	☐
18. Root cause, extent of condition, rectification and linked issues	☐
19. Decision-maker, date and reasons	☐

Appendix B. Reportable situation decision table

Work down the table. Stop at the first row that answers 'Report'. Record the reasons for every answer.

Step	Question	If yes	If no
1	Is there conduct that may be gross negligence or serious fraud by or a representative?	Report within 30 days (s912D(2))	Go to step 2
2	Are there reasonable grounds to believe there is a breach, or a likely breach, of a core obligation?	Go to step 4	Go to step 3
3	Is an investigation under way into whether there is a significant breach or likely breach, and has it continued for more than 60 days?	Report the investigation within 30 days of day 61; report the outcome when it ends	Keep investigating; track the 60-day trigger; record and rectify any non-core breach; go to step 7
4	Is the breach deemed significant (offence, civil penalty provision, credit key requirement, misleading or deceptive conduct, material loss or damage)?	Go to step 5	Go to step 6

Step	Question	If yes	If no
5	Does an exclusion in the regulations or Instrument 2024/620 apply, with every condition met, and no other deeming category applies?	Go to step 6	Report within 30 days
6	Having regard to all the s912D(5) / s50A(5) factors, is the breach significant?	Report within 30 days	Record as not reportable, with reasons; go to step 7
7	Is this a further situation with the same or substantially similar circumstances as one already reported?	Report within 90 days, by update where possible (Instrument 2024/620 s7)	Not applicable
8	Do we have reasonable grounds to believe an individual adviser or mortgage broker of another licensee is involved in a reportable situation?	Report within 30 days and copy the other licensee (s912DAB; s50C)	No report about another licensee
9	In every case: do the notify, investigate and remediate obligations, APRA, DDO, FAR, AUSTRAC, OAIC or other notifications apply?	Notify within each deadline (sections 16 to 18)	Record the assessment

Appendix C. Obligations register fields

Field	Description
Obligation ID and title	Unique reference and short name
Source	Act and section, regulation, prudential standard and paragraph, ASIC instrument, licence condition, code clause, contract or internal policy
Obligation summary	Plain-English description of what must be done, by whom and by when
Type	Mandatory (law, regulation, licence) or voluntary (code, contract, policy)
Core obligation?	Whether it is a core obligation under s912D(3) / s50A(3); whether it is a civil penalty provision or offence
Regulator	ASIC, APRA, AUSTRAC, OAIC, ACCC, AFCA, code compliance committee or other
Applies to	Legal entities, licences, products, business units and processes
Obligation owner	Named accountable senior manager (and accountable person under FAR, if applicable)
Controls	Key preventive, detective and corrective controls that meet the obligation, with control owners
Compliance risk rating	Critical, High, Medium or Low, with rationale
Monitoring and testing	Attestation frequency, last test date, result and next test date
Linked items	Risks, policies, procedures, incidents, breaches and issues
Regulatory change	Pending changes, effective dates and implementation actions
Reporting deadlines	Any notification or periodic reporting deadlines attached to the obligation
Review history	Date last reviewed and by whom; changes made

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.](#)