APRA CPS 234 — Information Security Readiness Assessment Report

Readiness assessment against APRA Prudential Standard CPS 234 and CPG 234

Organisation / system in scope	Southern Mutual Bank (fictional) / Core banking and customer channels
Framework	APRA CPS 234 (Information Security) · APRA · Prudential Standard CPS 234
Report type	CPS 234 readiness assessment — documentary review as at the assessment date
Assessment basis / period	As at 2026-11-09
Controls assessed	26
Evidence-led coverage	0 of 26 reached a verdict from evidence
Evidence reach	17 of 26 controls carry uploaded evidence (0 of those also carry a live signal); 9 carry neither
Report number	CS-SMB-2026-001
Report lifecycle / status	Sample report for a fictional organisation — not issued to a client
Generated (UTC)	2026-11-09T09:00:00Z

Important — scope and limitation of this report. This is a CyberSentien readiness assessment aligned to APRA CPS 234 / CPG 234. It supports the entity's own assurance and Board reporting; it is not an independent assurance engagement and does NOT constitute APRA approval.

Contents

§	Section
—	Document control, governance and issuance
—	Report format and standard alignment
—	How to read the results
—	Executive summary
—	What the engine did
1	Roles & responsibilities
2	Information security capability
3	Policy framework
4	Information-asset identification & classification
5	Implementation of controls
6	Incident management
7	Testing control effectiveness
8	Internal audit
9	APRA notification
10	Evidence freshness statement
11	AI assurance statement
12	APRA CPS 234 (Information Security) readiness conclusion
13	Risk ratings and remediation plan
—	Assessor statement
A–E	Appendices, opt-in — client dialogue, team communications, CISSP governance registers, assurance dialogue, controls excluded from assessment. Each carries a fixed letter and appears only where this engagement has that content, so the letters present below may not run consecutively.
F	Appendix — evidence to collect next (each control the AI review held back)

Section numbers match the headings used throughout this report.

Document control, governance and issuance

Report number	CS-SMB-2026-001
Report version	1.0
Report lifecycle / status	Sample report for a fictional organisation — not issued to a client
Assessment lead	Alex Morgan (fictional)
Reviewer	Priya Nair (fictional)
Approver	Daniel Okafor (fictional)
Review date	2026-11-10
Approval date	2026-11-10
Conflict-of-interest statement	No conflict of interest declared.
Distribution / reliance	For discussion with prospective clients and reviewers. The organisation, people and evidence in this report are fictional.
External issue approved	No — the quality gate blocks external issue: 0 of 26 controls reached a verdict from evidence

Sign-off chain (append-only, hash-linked): 3 entries — verified intact: prepared by Alex Morgan (fictional) (Lead assessor) on 2026-11-10; reviewed by Priya Nair (fictional) (Quality reviewer) on 2026-11-10; approved by Daniel Okafor (fictional) (Engagement director) on 2026-11-10.

How evidence is credited in this report

A control is shown as met only where an automated system check passed, or where an AI review that has passed an accuracy test for that framework credited it. Where AI credits are off for a framework, its documents are listed as candidate evidence for assessor review, with the reason.

AI credits on for CPS 234: at least 95% correct (9 wrong in 319 tested). The AI review read every control with a document cited against it, whatever the document's type. A control is shown as a credit only where the AI review confirmed it, with the passage it rests on; a control the documents alone did not show to be met is credited as partially met at most. Where the AI review did not confirm a control, it stays candidate evidence for assessor review, and a control with no document cited has nothing for the review to read. Each control's row says what the AI review found: confirmed; not shown, where the review found the documents cited do not show the control; a close call, which an assessor decides; or no evidence found, where no document is cited.

In this sample the AI review ran on a rented GPU over the fictional documents only. For a client it runs on hardware the client operates, or on a sovereign GPU the client arranges.

Controls in this report shown as candidate evidence for assessor review rather than as credits: 15 not confirmed by the AI review. Each lists its candidates and the reason.

Report format and standard alignment

Obligation pack / sources	APRA CPS 234 (Information Security) · APRA
Version	Prudential Standard CPS 234
Report format followed	CPS 234 readiness assessment — documentary review as at the assessment date
Primary source cited	https://www.apra.gov.au/information-security
Source access	public

This report follows CyberSentien's own reporting structure for APRA CPS 234 (Information Security). No published report template from the standard's own body is cited for it, so these sections are CyberSentien's, not a format issued by that body. 7 of the 9 sections below carry the framework's own structure by name; the rest are CyberSentien's. Sections covered:

1. Roles & responsibilities
2. Information security capability
3. Policy framework
4. Information-asset identification & classification
5. Implementation of controls
6. Incident management
7. Testing control effectiveness
8. Internal audit
9. APRA notification

Companion artefacts in this framework's report family: CPS 234 readiness assessment report, material information-asset register, control design assessment, operating-effectiveness report, third-party assurance report, incident-readiness report, board/senior-management deficiency report.

How to read the results

Every control in this report carries one of the results below. They are assigned by the assessment spine from the evidence actually cited — never by hand, and never inferred from the absence of evidence.

Result	What it means	Counts as an adverse finding
Implemented / operating effectively	Evidence was cited and supports the control operating as required.	No
Partially implemented (exception)	Evidence was cited and supports the control only in part — an exception is recorded against it.	Yes
Not met / gap	Evidence, or an adverse signal, shows the control is not in place or is not operating.	Yes
Evidenced but stale	Evidence was cited but is older than the freshness threshold, so it is not treated as current assurance.	Yes
No visibility	The assessment could not observe this control at all — the source that would show it was unreachable.	Yes
Insufficient evidence	What was supplied does not establish the control either way. This is a gap in the evidence, not a finding against the control.	No
Manual assessment required	No automated signal and no uploaded evidence reach this control; it is for the assessor to judge directly.	No
Candidate evidence — assessor review	Evidence reached this control but it is not presented as a credit: either documents were aligned to it and are listed as candidates (the framework is not lifted by measurement, its admission gate is unmet, or AI credits are off for it until proven), or connector checks tested only some of the requirements the control bundles (each tested requirement is listed with its result, and the rest are listed as remaining requirements for assessor review). An assessor must confirm. This is neither a gap nor a finding.	No

A control with no evidence is NOT reported as a failure. "Insufficient evidence" and "Manual assessment required" say the assessment could not reach a verdict from what was supplied; only an adverse signal, or evidence that states the control is absent, produces "Not met / gap".

What a cited document is. The documents listed against a control are the evidence this engine's matcher aligned to it most strongly, ranked by that matcher. They are the assessor's starting point, not a finding that each document addresses that control: confirming relevance is an assessor judgement, and where a citation is off-subject the control's result should be read as resting on the assessor's review rather than on the citation alone.

Not every catalogued row is an obligation this engine can assess. Of 36 catalogued controls, 10 are excluded from assessment and from every count in this report; the remaining 26 are graded above. Nothing is dropped — each excluded control is listed with its reason in the appendix “Controls excluded from assessment”. Reasons for this framework: Definitions — not an obligation on the entity; The instrument stating how it is to be read — not an obligation on the entity; The instrument stating what it applies to — not an obligation on the entity; The instrument stating when it commences — not an obligation on the entity.

Executive summary

—	0	9
implemented (no evidence-led result yet)	gaps / not met	manual assessment required

Against APRA CPS 234 (Information Security), 0 of 26 controls were assessed from evidence (continuous signals and the assessor's uploaded evidence), of which 0 are implemented, 0 partially, and 0 are gaps. 9 controls have no automated signal or uploaded evidence and require assessor review. A further 17 are outstanding: 13 candidate evidence — assessor review; 4 insufficient evidence — assessed, not established. All figures are evidence-led; nothing is asserted as compliant without evidence (no false green).

What the engine did

Every number below is counted from this report's own results; nothing is estimated. The document matcher reads the evidence first and puts controls forward; the AI review then reads each one against the documents cited and either confirms it, refuses it, or leaves it as a close call for an assessor. A refused or close-call control is not a failed control: it is candidate evidence for assessor review, and the appendix "Evidence to collect next" says what would show it.

What was counted	Result
Documents in the evidence pack (all fictional; the same pack for all four sample reports)	76
Controls assessed	26
Controls with a document cited against them	17
Controls the document matcher put forward from the documents, each read by the AI review	17
Confirmed by the AI review and shown as a credit, with the passage it rests on	0
Refused by the AI review: the documents cited do not show the control	8
Close calls the AI review left for an assessor to decide	9
Controls with no document cited, so nothing for the AI review to read	9
The AI review's tested accuracy for CPS 234	310 of 319 credits right (97.2%) in an independent test on fictional evidence

1. Roles & responsibilities

The controls this assessment holds under "Roles and responsibilities", with the requirement each states, the evidence cited for it and its result — the same spine the whole-catalogue matrix reads, shown here as this theme alone. Every control in this catalogue is reported under exactly one section of this report. Each row is a requirement of the framework, assessed from the evidence route stated on the row; the entity's own controls have not been registered against the requirements and no population was sampled, so these results are readiness findings for the assessor, not tests of the entity's controls.

Roles and responsibilities (2)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-13	Roles and responsibilities	No automated signal or uploaded evidence — assessor review required. **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.
cl-14	Roles and responsibilities	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** close call (an assessor decides)	029_security_governance_committee_charter.pdf · `e59df87042d8…` *"4.6.3 Roles and responsibilities shall align to the three-lines-of-defence model, with first-line ownership, second-line oversight and third-line independent assurance."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Candidate evidence — assessor review	Provide evidence to enable an evidence-led result.

*How to read this table: one row per control, grouped under the control area named in the heading above each block. **Name / area** is the control's own name where this framework's catalogue gives one, and the control area otherwise — some catalogues name their controls only by identifier, and repeating the identifier or the area heading beside it would tell a reader nothing they do not already have on the line.*

Requirement text for the controls reported above.

cl-13

The Board4 of an APRA -regulated entity (Board) is ultimately responsible for the information security of the entity. The Board must ensure that the entity maintains information security in a manner commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity .5

cl-14

An APRA -regulated entity must clearly define t he information security -related roles and responsibilities of the Board , senior management , governing bodies and individuals with responsibilit y for decision -making, approval, oversight, operations and other information security functions.6

2. Information security capability

The controls this assessment holds under "Information security capability", with the requirement each states, the evidence cited for it and its result — the same spine the whole-catalogue matrix reads, shown here as this theme alone. Every control in this catalogue is reported under exactly one section of this report. Each row is a requirement of the framework, assessed from the evidence route stated on the row; the entity's own controls have not been registered against the requirements and no population was sampled, so these results are readiness findings for the assessor, not tests of the entity's controls.

Information security capability (3)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-15	Information security capability	No automated signal or uploaded evidence — assessor review required. **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-16	Information security capability	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** close call (an assessor decides)	020_vendor_security_assessment_standard.pdf · `0cb5dc4bae48…` 116_vendor_assurance_evidence_soc_2_summary_microsoft_q2_2026.pdf · `cc7f4de7a50d…` 206_vendor_assurance_evidence_soc_2_summary_microsoft_q3_2025.pdf · `dbd97aab0e7b…` *"Summary of results Supplier Microsoft Report SOC 2 Type II, 12-month period, unqualified opinion Complementary user entity controls 7 — mapped to our controls Sub-service organisations 2 — carve-out method 3."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Candidate evidence — assessor review	Provide evidence to enable an evidence-led result.
cl-17	Information security capability	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** close call (an assessor decides)	104_vulnerability_scan_report_core_banking_temenos_t24_q2_2026.pdf · `57d272bb1f0c…` 112_patch_compliance_report_core_banking_temenos_t24_q2_2026.pdf · `159ccb7ae035…` *"Summary of results Hosts scanned (authenticated) 412 Critical / high vulnerabilities open 3 / 11 Remediated within SLA 91% Scan coverage of estate 98.6% 3."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Candidate evidence — assessor review	Provide evidence to enable an evidence-led result.

*How to read this table: one row per control, grouped under the control area named in the heading above each block. **Name / area** is the control's own name where this framework's catalogue gives one, and the control area otherwise — some catalogues name their controls only by identifier, and repeating the identifier or the area heading beside it would tell a reader nothing they do not already have on the line.*

Requirement text for the controls reported above.

cl-15

An APRA -regulated entity must maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound ope ration of the entity .

cl-16

Where information asset s are managed by a related party or third party, the APRA -regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets .7

cl-17

An APRA -regulated entity must actively maintain its information security capability with respect to changes in vulnerabilities and threat s, including those resulting from changes to information assets or its business environment .

2a. Control coverage by domain

The assessed control set grouped by CyberSentien's analytical control domains — where coverage and effectiveness sit across access, data, network, threat detection, incident response and the supporting governance, physical, personnel, asset, application and supply-chain domains. **This is a management lens, not this framework's own grouping**: it is derived from each control's identifier, family and stored text, it reproduces no standard's taxonomy, and its domain names are not the catalogue groups used by the control assessment and the residual register elsewhere in this report — so a domain here and a group there may share a name and count

different controls.

Data Protection	0 of 1 Implemented / operating effectively (0%) — 1 Candidate evidence — assessor review
Threat Detection	0 of 3 Implemented / operating effectively (0%) — 1 Insufficient evidence, 1 Manual assessment required, 1 Candidate evidence — assessor review
Incident Response	0 of 6 Implemented / operating effectively (0%) — 2 Insufficient evidence, 4 Candidate evidence — assessor review
Governance & Risk	0 of 6 Implemented / operating effectively (0%) — 1 Insufficient evidence, 3 Manual assessment required, 2 Candidate evidence — assessor review
Personnel Security	0 of 1 Implemented / operating effectively (0%) — 1 Manual assessment required
Asset & Configuration	0 of 5 Implemented / operating effectively (0%) — 2 Manual assessment required, 3 Candidate evidence — assessor review
Supply Chain / Third-Party	0 of 2 Implemented / operating effectively (0%) — 2 Candidate evidence — assessor review
Other	0 of 2 Implemented / operating effectively (0%) — 2 Manual assessment required

2b. Security awareness and culture

The assessment captured training and awareness evidence for this submission. This supports bounded reporting on security awareness activity, but does not by itself establish a broader positive security-culture maturity conclusion beyond the preserved artefacts.

This is a statement about what the engagement CAPTURED, derived from the evidence set itself. The controls that require awareness training are assessed on their own evidence in the control assessment, and their results are not restated here.

3. Policy framework

The controls this assessment holds under "Policy framework", with the requirement each states, the evidence cited for it and its result — the same spine the whole-catalogue matrix reads, shown here as this theme alone. Every control in this catalogue is reported under exactly one section of this report. Each row is a requirement of the framework, assessed from the evidence route stated on the row; the entity's own controls have not been registered against the requirements and no population was sampled, so these results are readiness findings for the assessor, not tests of the entity's controls.

Policy framework (2)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-18	Policy framework	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-19	Policy framework	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** close call (an assessor decides)	002_access_control_policy.pdf · `b0d755704774…` 019_third_party_risk_management_policy.pdf · `dc41ed8ba096…` 001_information_security_policy.pdf · `19b799381535…` *"Scope This document applies to all employees, contractors, temporary staff and third parties acting for Southern Mutual Bank, and to all information assets, systems and environments it operates or operates on its behalf — on-premise, cloud (AWS/Azure), SaaS and outsourced services."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Candidate evidence — assessor review	Provide evidence to enable an evidence-led result.

*How to read this table: one row per control, grouped under the control area named in the heading above each block. **Name / area** is the control's own name where this framework's catalogue gives one, and the control area otherwise — some catalogues name their controls only by identifier, and repeating the identifier or the area heading beside it would tell a reader nothing they do not already have on the line.*

Requirement text for the controls reported above.

cl-18

An APRA -regulated entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.

cl-19

An APRA -regulated entity ’s information security policy framework must provide direction on the responsibilities of all parties who have an obligation to maintain information security .8

4. Information-asset identification & classification

The controls this assessment holds under "Identification & classification", with the requirement each states, the evidence cited for it and its result — the same spine the whole-catalogue matrix reads, shown here as this theme alone. Every control in this catalogue is reported under exactly one section of this report. Each row is a requirement of the framework, assessed from the evidence route stated on the row; the entity's own controls have not been registered against the requirements and no population was sampled, so these results are readiness findings for the assessor, not tests of the entity's controls.

Identification & classification (1)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-20	Identification & classification	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** not shown by the documents cited	023_data_classification_handling_standard.pdf · `056d78ec3f06…` *"Scope This document applies to all employees, contractors, temporary staff and third parties acting for Southern Mutual Bank, and to all information assets, systems and environments it operates or operates on its behalf — on-premise, cloud (AWS/Azure), SaaS and outsourced services."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Candidate evidence — assessor review	Provide evidence to enable an evidence-led result.

*How to read this table: one row per control, grouped under the control area named in the heading above each block. **Name / area** is the control's own name where this framework's catalogue gives one, and the control area otherwise — some catalogues name their controls only by identifier, and repeating the identifier or the area heading beside it would tell a reader nothing they do not already have on the line.*

Requirement text for the controls reported above.

cl-20

An APRA -regulated entity must classify its information assets , including those managed by related parties and third parties, by criticality and sensitivity . This classification must reflect the degree to which an information security incident affecting an information asset has the potential to affect , financially or non - financially, the entity or the interests of depositors, policyholders , beneficiaries or other customers .

4a. Assessment scope and system boundary

Boundary summary	Internet banking portal, core banking platform and Microsoft 365 tenant in scope; the card processor is a third party outside the boundary.
Control baseline	Commercial-in-confidence

Consultant-defined in/out-of-scope topology · reviewed and confirmed · system: Core banking and customer channels

Boundary element	Position
Internet banking portal (Application)	In scope
Core banking platform (Application)	In scope
Microsoft 365 tenant (Cloud service)	In scope
Card processor (Third party)	Out of scope

5. Implementation of controls

The controls this assessment holds under "Implementation of controls", with the requirement each states, the evidence cited for it and its result — the same spine the whole-catalogue matrix reads, shown here as this theme alone. Every control in this catalogue is reported under exactly one section of this report. Each row is a requirement of the framework, assessed from the evidence route stated on the row; the entity's own controls have not been registered against the requirements and no population was sampled, so these results are readiness findings for the assessor, not tests of the entity's controls.

Implementation of controls (2)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-21	Implementation of controls	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.
cl-22	Implementation of controls	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.

*How to read this table: one row per control, grouped under the control area named in the heading above each block. **Name / area** is the control's own name where this framework's catalogue gives one, and the control area otherwise — some catalogues name their controls only by identifier, and repeating the identifier or the area heading beside it would tell a reader nothing they do not already have on the line.*

Requirement text for the controls reported above.

cl-21

An APRA -regulated entity must have information security controls to protect its information assets , including those managed by related parties and third parties , that are implemented in a timely manner and that are commensurate with: (a) vulnerabilities and threats to the information assets ; (b) the criticality and sensitivity of the information asset s; (c) the stage at which the information asset s are within their life-cycle;9 and (d) the potential consequences of an information security incident .

cl-22

Where an APRA -regulated entity’s information assets are managed by a related party or third part y, the APRA -regulated entity must evaluate the design of that party’s information security controls that protects the information assets of the APRA -regulated entity .10

5a. Detailed control assessment (controls not reported under a theme above)

Every control assessed individually: the requirement, the test/assessment performed, the cited evidence with its SHA-256 integrity hash, the result, and the finding & recommendation where adverse. Control text is shown in full; the evidence line lists the first four cited artefacts and states how many more there are. Each row is a requirement of the framework, assessed from the evidence route stated on the row; the entity's own controls have not been registered against the requirements and no population was sampled, so these results are readiness findings for the assessor, not tests of the entity's controls.

Application & interpretation (2)

cl-6 — Candidate evidence — assessor review

Requirement. Where an APRA -regulated entity’s information assets are managed by a third party, the requirements in this Prudential Standard will apply in relation to those information assets from the ear lier of the next renewal date of the contract with the third party or 1 July 202 0. Interpretation

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Not shown. The AI review read the documents cited and found that they do not show this control.

Evidence. 020_vendor_security_assessment_standard.pdf `0cb5dc4bae48`…;
116_vendor_assurance_evidence_soc_2_summary_microsoft_q2_2026.pdf `cc7f4de7a50d`…;
206_vendor_assurance_evidence_soc_2_summary_microsoft_q3_2025.pdf `dbd97aab0e7b`…

cl-10 — Manual assessment required

Requirement. For the purposes of this Prudential Standard: ‘group’ means a Level 2 group or a Level 3 group , as relevant; ‘Head of a group’ means a Level 2 Head or Level 3 Head , as relevant; ‘Level 2 group’ means the entities that comprise: (a) Level 2 as def ined in APS 001; or (b) a Level 2 insurance group as defined in GPS 001; ‘Level 2 Head’ means: (a) where an ADI that is a member of a Level 2 group is not a subsidiary of an authorised banking NOHC or another ADI, that ADI; (b) where an ADI that is a member of a Level 2 group is a subsidiary of an authorised banking NOHC, that authorised banking NOHC; or (c) the parent entity of a Level 2 insurance group as defined in GPS 001.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. No evidence found. No document in the evidence pack is cited for this control, so there was nothing for the AI review to read.

Action. Provide evidence (a live signal or an uploaded document) to enable an evidence-led result.

5b. Collection & intelligence basis

Evidence is collected continuously from connected sources, normalised to one canonical model, and mapped to this framework's controls via the shared control-signal spine.

Platform connector capability. 57 of 62 connector types the platform supports collect at deep+ depth (deep 54, standard 3, trench 3, shallow 2). A connected source is auto-polled and its canonical records feed this framework through the spine. **In this engagement no live signal reached any control**, so this describes what the platform can collect once a source is connected. It is not evidence in this report.

Reading. Reader coverage for this framework — cited (document, control) pairs read: 36 of 36. Credited with a quoted passage: 0. Shown as candidate evidence for assessor review: 17, of which 0 were credited by the deterministic assessment and appear here for confirmation rather than as gaps.

5c. Catalogue controls not reported above

The catalogue controls not reported under a theme section above, grouped by domain. For each: the continuous test performed, the cited evidence with its SHA-256 integrity hash, the result over the assessment, and the finding/remediation where adverse. Control text is shown in full; the evidence column lists the first three cited artefacts and states how many more there are. Each row is a requirement of the framework, assessed from the evidence route stated on the row; the entity's own controls have not been registered against the requirements and no population was sampled, so these results are readiness findings for the assessor, not tests of the entity's controls.

Application & interpretation (2)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-6	Application & interpretation	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** not shown by the documents cited	020_vendor_security_assessment_standard.pdf · `0cb5dc4bae48`… 116_vendor_assurance_evidence_soc_2_summary_microsoft_q2_2026.pdf · `cc7f4de7a50d`… 206_vendor_assurance_evidence_soc_2_summary_microsoft_q3_2025.pdf · `dbd97aab0e7b`… *“Results were produced from the system of record and the tooling named below; exceptions are listed with an owner and a due date and are tracked to closure by the control owner, with second-line oversight.”* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Candidate evidence — assessor review	Provide evidence to enable an evidence-led result.
cl-10	Application & interpretation	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.

*How to read this table: one row per control, grouped under the control area named in the heading above each block. **Name / area** is the control's own name where this framework's catalogue gives one, and the control area otherwise — some catalogues name their controls only by identifier, and repeating the identifier or the area heading beside it would tell a reader nothing they do not already have on the line.*

6. Incident management

The controls this assessment holds under "Incident management", with the requirement each states, the evidence cited for it and its result — the same spine the whole-catalogue matrix reads, shown here as this theme alone. Every control in this catalogue is reported under exactly one section of this report. Each row is a requirement of the framework, assessed from the evidence route stated on the row; the entity's own controls have not been registered against the requirements and no population was sampled, so these results are readiness findings for the assessor, not tests of the entity's controls.

Incident management (4)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-23	Incident management	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** close call (an assessor decides)	208_incident_post_mortem_q3_2025.pdf · `72971ff13676…` 118_incident_post_mortem_q2_2026.pdf · `ee3caab338c2…` *"Summary of results Security incident INC-2026-0142 — business email compromise, severity 2 Time to detect / contain 41 min / 2h 10m Customer impact None confirmed Notifications APRA CPS 234 within 72h; OAIC assessment — not eligible 3."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Insufficient evidence	Provide evidence to enable an evidence-led result.
cl-24	Incident management	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** not shown by the documents cited	208_incident_post_mortem_q3_2025.pdf · `72971ff13676…` 118_incident_post_mortem_q2_2026.pdf · `ee3caab338c2…` *"Summary of results Security incident INC-2026-0142 — business email compromise, severity 2 Time to detect / contain 41 min / 2h 10m Customer impact None confirmed Notifications APRA CPS 234 within 72h; OAIC assessment — not eligible 3."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Insufficient evidence	Provide evidence to enable an evidence-led result.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-25	Incident management	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** close call (an assessor decides)	011_data_breach_response_procedure.pdf · `4bc5e0e094ad…` 010_incident_response_plan.pdf · `42ae39730590…` 008_logging_monitoring_policy.pdf · `808a97e670d8…` *"Scope This document applies to all employees, contractors, temporary staff and third parties acting for Southern Mutual Bank, and to all information assets, systems and environments it operates or operates on its behalf — on-premise, cloud (AWS/Azure), SaaS and outsourced services."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Candidate evidence — assessor review	Provide evidence to enable an evidence-led result.
cl-26	Incident management	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** not shown by the documents cited	032_operational_resilience_policy_cps_230.pdf · `4027f4cd46d7…` 010_incident_response_plan.pdf · `42ae39730590…` 013_disaster_recovery_plan.pdf · `43e28b398d1d…` *+ 1 more cited (see the evidence register)* *"4.3 Continuity and scenario testing 4.3.1 Disaster-recovery plans shall be maintained and exercised for critical systems at least annually."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Candidate evidence — assessor review	Provide evidence to enable an evidence-led result.

*How to read this table: one row per control, grouped under the control area named in the heading above each block. **Name / area** is the control's own name where this framework's catalogue gives one, and the control area otherwise — some catalogues name their controls only by identifier, and repeating the identifier or the area heading beside it would tell a reader nothing they do not already have on the line.*

Requirement text for the controls reported above.

cl-23

An APRA -regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner.

cl-24

An APRA -regulated entity must maintain plans to respond to information security incidents that the entity considers could plausibly occur (information security response plans) .

cl-25

An APRA -regulated entity's information security response plan s must include the mechanisms in place for : (a) manag ing all relevant stages of an incident , from detection to post-incident review ; and (b) escalation and reporting of information security incidents to the Board, other governing bodies and individuals responsible for information security incident management and oversight , as appropriate .

cl-26

An APRA -regulated entity must annually review and test its information security response plans to ensure they remain effective and fit -for-purpose .

6a. Changes during the period (drift)

No assessment baseline has been captured for this scope, so no drift comparison was performed. This section reports control-relevant changes detected against a captured baseline; with no baseline there is nothing to compare against, and the absence of changes below is not evidence that none occurred. Capture a baseline to make subsequent assessments drift-aware.

7. Testing control effectiveness

The controls this assessment holds under "Testing control effectiveness", with the requirement each states, the evidence cited for it and its result — the same spine the whole-catalogue matrix reads, shown here as this theme alone. Every control in this catalogue is reported under exactly one section of this report. Each row is a requirement of the framework, assessed from the evidence route stated on the row; the entity's own controls have not been registered against the requirements and no population was sampled, so these results are readiness findings for the assessor, not tests of the entity's controls.

Testing control effectiveness (5)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-27	Testing control effectiveness	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** close call (an assessor decides)	052_audit_findings_risk_treatment_register.pdf · `5cc25603c344`… *"Register entries ID Risk / finding Likelihood x impact Risk owner Treatment plan Residual risk / status AUD-001 Internal audit finding — privileged access recertification evidence incomplete Possible x Major = High Mei-Lin Tan Compensating control in place; risk assessment refreshed High — OUTSIDE APPETITE, escalated to Board Risk Committee AUD-002 External audit finding — backup restoration test"* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Insufficient evidence	Provide evidence to enable an evidence-led result.
cl-28	Testing control effectiveness	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** not shown by the documents cited	020_vendor_security_assessment_standard.pdf · `0cb5dc4bae48`… 116_vendor_assurance_evidence_soc_2_summary_microsoft_q2_2026.pdf · `cc7f4de7a50d`… 206_vendor_assurance_evidence_soc_2_summary_microsoft_q3_2025.pdf · `dbd97aab0e7b`… *"Summary of results Supplier Microsoft Report SOC 2 Type II, 12-month period, unqualified opinion Complementary user entity controls 7 — mapped to our controls Sub-service organisations 2 — carve-out method 3."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Candidate evidence — assessor review	Provide evidence to enable an evidence-led result.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-29	Testing control effectiveness	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.
cl-30	Testing control effectiveness	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.
cl-31	Testing control effectiveness	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.

*How to read this table: one row per control, grouped under the control area named in the heading above each block. **Name / area** is the control's own name where this framework's catalogue gives one, and the control area otherwise — some catalogues name their controls only by identifier, and repeating the identifier or the area heading beside it would tell a reader nothing they do not already have on the line.*

Requirement text for the controls reported above.

cl-27

An APRA -regulated entity must test the effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with: (a) the rate at which the vulnerabilities and threats change; (b) the criticality and sensitivity of the information asset; (c) the consequence s of an information security incident ; (d) the risks associated with exposure to environments where the APRA - regulated entity is unable to enforce its information security polic ies;11 and (e) the materiality and frequency of change to information assets .

cl-28

Where an APRA -regulated entity’s information assets are managed by a related party or a third party , and the APRA -regulated entity is reliant on that party’s information security control testin g, the APRA -regulated entity must assess whether the nature and frequency of testing of controls in respect of those information assets is commensurate with paragraph s 27(a) to 27(e) of this Prudential Standard .12

cl-29

An APRA -regulated entity must escalate and report to the Board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner.

cl-30

An APRA -regulated entity must ensure that testing is conducted by appropriately skilled and functionally independent specialists.

cl-31

An APRA -regulated entity must review the sufficiency of the testing program at least annually or when there is a material change to information assets or the business environment.

7a. Assessment methodology and evidence collection

Controls were assessed from two evidence streams, crosswalked from the one assessment: (a) continuous, read-only signals (Microsoft 365 collectors, connectors and the governance register), and (b) the assessor's uploaded evidence — routed from the ISM assessment via a validated crosswalk so the same evidence is applied to this framework's controls. Each control's test is stated on the control itself and is derived from the route that answered it, never assumed: a documentary review of the uploaded evidence as at the assessment date. No live

collector signal reached any of the 17 controls assessed here, so nothing in this report rests on continuous validation. A further 9 controls had no evidence route at all and are for the assessor to judge directly. The result is the validation state; exceptions are failed/partial/no-visibility controls.

Sampling and population. For automated controls the population is the full live signal set (census, not sample). For document-evidenced controls, the cited artefact(s) are inspected and hash-stamped. Controls with neither a signal nor uploaded evidence are reported honestly as 'manual assessment required' — never assumed compliant.

Control identifiers are referenced as they appear in this framework's canonical pack. Whether the requirement text is CyberSentien's own wording or reproduces the authority's published text has not yet been classified for this framework (see its authority record); no claim about that is made here. Verdicts are deterministic and human-owned — the assessor confirms.

7b. Pillar alignment and reporting KPIs

Each pillar of the framework's own structure reports its configured lead KPI — chosen per engagement on the console, defaulting to the market-researched metric for the pillar's theme. Every KPI is computed solely from the evidence in scope for that pillar; pillars with no evidence report honest zeros.

Pillar	Lead KPI	Value	Verified	Evidence on file	At risk	Evidence gap / no visibility	Unassessed
Application & interpretation	Verified — % of catalogue	0% of catalogue verified	0/2	1	0	0	1
Roles and responsibilities	Evidence on file — % of catalogue	50% of catalogue have evidence on file · 0 verified	0/2	1	0	0	1
Information security capability	Verified — % of catalogue	0% of catalogue verified	0/3	2	0	0	1
Policy framework	Evidence on file — % of catalogue	50% of catalogue have evidence on file · 0 verified	0/2	1	0	0	1
Identification & classification	Verified — % of catalogue	0% of catalogue verified	0/1	1	0	0	0
Implementation of controls	Verified — % of catalogue	— (no evidence yet)	0/2	0	0	0	2
Incident management	Freshness — % current (30-day window)	— (no evidence dates recorded)	0/4	4	0	2	0
Testing control effectiveness	Verified — % of catalogue	0% of catalogue verified	0/5	2	0	1	3
Internal audit	Verified — % of catalogue	0% of catalogue verified	0/3	3	0	1	0
APRA notification	Freshness — % current (30-day window)	— (no evidence dates recorded)	0/2	2	0	0	0

Column headings, in the results vocabulary defined on page 2: **Verified** = Implemented / operating effectively; **Evidence on file** = Implemented / operating effectively, Partially implemented (exception), Not met / gap, Evidenced but stale, Insufficient evidence and Candidate evidence — assessor review; **At risk** = Not met / gap and Evidenced but stale; **Evidence gap / no visibility** = Insufficient evidence and No visibility; **Unassessed** = Manual assessment required. Each column is a COUNT of controls with that result, not a result in its own right.

How to read this table: lead KPI = the engagement's configured pillar metric (change it on the console by clicking the tile reading); denominators are the full pillar catalogue — unassessed controls are counted, never hidden (no false green). The "Evidence gap / no visibility" column holds two distinct results: 4 insufficient evidence (evidence was supplied and does not establish the control — not an adverse finding) and 0 no visibility (the source that would show the control was unreachable — an adverse finding). Each control's own result is printed in the control matrix.

8. Internal audit

The controls this assessment holds under "Internal audit", with the requirement each states, the evidence cited for it and its result — the same spine the whole-catalogue matrix reads, shown here as this theme alone. Every control in this catalogue is reported under exactly one section of this report. Each row is a requirement of the framework, assessed from the evidence route stated on the row; the entity's own controls have not been registered against the requirements and no population was sampled, so these results are readiness findings for the assessor, not tests of the entity's controls.

Internal audit (3)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-32	Internal audit	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** close call (an assessor decides)	052_audit_findings_risk_treatment_register.pdf · `5cc25603c344…` *"overdue Possible x Major = High Priya Sharma Compensati ng control in place; risk assessment refreshed Low — closed AUD-003 Regulatory review — incident notification timeframe not evidenced Possible x Moderate = Medium James O'Connor Remediatio n plan tracked to closure in the risk register Low — closed AUD-004 Internal audit — firewall rule review not performed for two quarters Rare x Severe ="* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Candidate evidence — assessor review	Provide evidence to enable an evidence-led result.
cl-33	Internal audit	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** not shown by the documents cited	052_audit_findings_risk_treatment_register.pdf · `5cc25603c344…` *"AUD-006 Internal audit — supplier assurance reports not reviewed Rare x Severe = Medium Aisha Khan Risk treatment: control uplift funded, target 27 Jan 2027 Low — closed AUD-007 Penetration test — high finding open beyond SLA Possible x Major = High Laura Mendez Risk acceptance by accountable executive, reviewed quarterly Medium — within risk appetite AUD-008 Internal audit — security awareness"* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Insufficient evidence	Provide evidence to enable an evidence-led result.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-34	Internal audit	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** not shown by the documents cited	020_vendor_security_assessment_standard.pdf · `0cb5dc4bae48…` *"4.8.4 Independent assurance (internal audit / external assessment) shall periodically test design and operating effectiveness; findings shall be tracked to closure."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Candidate evidence — assessor review	Provide evidence to enable an evidence-led result.

*How to read this table: one row per control, grouped under the control area named in the heading above each block. **Name / area** is the control's own name where this framework's catalogue gives one, and the control area otherwise — some catalogues name their controls only by identifier, and repeating the identifier or the area heading beside it would tell a reader nothing they do not already have on the line.*

Requirement text for the controls reported above.

cl-32

An APRA -regulated entity 's internal audit activities must 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) .

cl-33

An APRA -regulated entity must ensure that the information security control assurance is provided by personnel appropria tely skilled in providing such assurance .

cl-34

An APRA -regulated entity's internal audit function must assess the information security control assurance provided by a related party or third party where: (a) an information security incident affecting the information assets has the potential to materially affect, financially or non -financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; and (b) internal audit intends to rely on the information security control assurance provided by the related party or third party .13

8a. Exceptions register

No control was found failed, partially met, stale or unobservable. **This is not a finding of compliance:** 26 of 26 controls are not yet demonstrated (they await evidence or assessor confirmation), and each carries a risk rating, an action, an owner and a target date in the "Risk ratings and remediation plan" section.

8b. Remediation plan

No adverse finding requires remediation. **This is not a finding of compliance:** 26 of 26 controls are not yet demonstrated (they await evidence or assessor confirmation), and each carries a risk rating, an action, an owner and a target date in the "Risk ratings and remediation plan" section.

8c. Evidence-request and remediation register (fast-track)

0 controls to remediate · 13 for the assessor to confirm (candidate evidence on file) · 9 to request from the client · 4 insufficient evidence — the same assessed controls reported throughout this report, grouped into the assessor's working lists.

Pillar	Action	Control	Label	Result
Application & interpretation	Assessor to confirm	cl-6	Application & interpretation	Candidate evidence — assessor review
Application & interpretation	Request from client	cl-10	Application & interpretation	Manual assessment required

Pillar	Action	Control	Label	Result
Roles and responsibilities	Assessor to confirm	cl-14	Roles and responsibilities	Candidate evidence — assessor review
Roles and responsibilities	Request from client	cl-13	Roles and responsibilities	Manual assessment required
Information security capability	Assessor to confirm	cl-16	Information security capability	Candidate evidence — assessor review
Information security capability	Assessor to confirm	cl-17	Information security capability	Candidate evidence — assessor review
Information security capability	Request from client	cl-15	Information security capability	Manual assessment required
Policy framework	Assessor to confirm	cl-19	Policy framework	Candidate evidence — assessor review
Policy framework	Request from client	cl-18	Policy framework	Manual assessment required
Identification & classification	Assessor to confirm	cl-20	Identification & classification	Candidate evidence — assessor review
Implementation of controls	Request from client	cl-21	Implementation of controls	Manual assessment required
Implementation of controls	Request from client	cl-22	Implementation of controls	Manual assessment required
Incident management	Assessor to confirm	cl-25	Incident management	Candidate evidence — assessor review
Incident management	Assessor to confirm	cl-26	Incident management	Candidate evidence — assessor review
Incident management	Re-evidence	cl-23	Incident management	Insufficient evidence
Incident management	Re-evidence	cl-24	Incident management	Insufficient evidence
Testing control effectiveness	Assessor to confirm	cl-28	Testing control effectiveness	Candidate evidence — assessor review
Testing control effectiveness	Request from client	cl-29	Testing control effectiveness	Manual assessment required
Testing control effectiveness	Request from client	cl-30	Testing control effectiveness	Manual assessment required
Testing control effectiveness	Request from client	cl-31	Testing control effectiveness	Manual assessment required
Testing control effectiveness	Re-evidence	cl-27	Testing control effectiveness	Insufficient evidence

Pillar	Action	Control	Label	Result
Internal audit	Assessor to confirm	cl-32	Internal audit	Candidate evidence — assessor review
Internal audit	Assessor to confirm	cl-34	Internal audit	Candidate evidence — assessor review
Internal audit	Re-evidence	cl-33	Internal audit	Insufficient evidence
APRA notification	Assessor to confirm	cl-35	APRA notification	Candidate evidence — assessor review
APRA notification	Assessor to confirm	cl-36	APRA notification	Candidate evidence — assessor review

How to read this table: the assessor's working lists, built from the results reported above and nowhere else — remediate rows are failed, stale or partially met controls; confirm rows have candidate evidence cited that an assessor must confirm; request rows are controls with no cited document and no live signal (the client PBC list); re-evidence rows lost visibility or drew insufficient evidence. Every row's result is the one this report assigns that control.

8d. Residual risk register

Residual ratings are deterministic defaults derived from the assessment; the assessor confirms the final rating, treatment and acceptance.

Catalogue group	Controls	Met	Not met	Partial	Not yet shown	Residual rating	Contributing controls
Application & interpretation	2	0	0	0	2	To be determined — default, assessor to confirm	cl-6, cl-10
Roles and responsibilities	2	0	0	0	2	To be determined — default, assessor to confirm	cl-13, cl-14
Information security capability	3	0	0	0	3	To be determined — default, assessor to confirm	cl-15, cl-16, cl-17
Policy framework	2	0	0	0	2	To be determined — default, assessor to confirm	cl-18, cl-19
Identification & classification	1	0	0	0	1	To be determined — default, assessor to confirm	cl-20
Implementation of controls	2	0	0	0	2	To be determined — default, assessor to confirm	cl-21, cl-22
Incident management	4	0	0	0	4	To be determined — default, assessor to confirm	cl-23, cl-24, cl-25, cl-26

Catalogue group	Controls	Met	Not met	Partial	Not yet shown	Residual rating	Contributing controls
Testing control effectiveness	5	0	0	0	5	To be determined — default, assessor to confirm	cl-27, cl-28, cl-29, cl-30, cl-31
Internal audit	3	0	0	0	3	To be determined — default, assessor to confirm	cl-32, cl-33, cl-34
APRA notification	2	0	0	0	2	To be determined — default, assessor to confirm	cl-35, cl-36

Column headings, in the results vocabulary defined on page 2: **Met** = Implemented / operating effectively; **Not met** = Not met / gap; **Partial** = Partially implemented (exception); **Not yet shown** = Insufficient evidence, Manual assessment required, Candidate evidence — assessor review, No visibility and Evidenced but stale. Each column is a COUNT of controls with that result, not a result in its own right.

Contributing controls are the open controls in that domain (not met, partial or not yet shown, up to eight) that drive its residual rating, named in this framework's own control identifiers so the reader can turn to them in the control assessment. A control that is not yet shown is listed because it is unevidenced rather than failed; it is not an adverse finding. A dash means no control in that domain is open.

8e. Quality gate and issuance readiness

Gate check	Status	Detail
Control catalogue assessed	PASS	26 controls assessed
Evidence-led coverage present	BLOCK	0 of 26 controls reached a verdict from evidence
System boundary captured	PASS	captured and reviewed
Evidence pack attached (source artefacts)	PASS	cited evidence present
Issuance governance complete (lead/reviewer/approver/sign-off)	BLOCK	blocked by the gate rows above

Gate decision: Controlled internal draft — fit for assessor review and discussion; NOT for external issue until the BLOCK items above are cleared and the report is signed off.

9. APRA notification

The controls this assessment holds under "APRA notification", with the requirement each states, the evidence cited for it and its result — the same spine the whole-catalogue matrix reads, shown here as this theme alone. Every control in this catalogue is reported under exactly one section of this report. Each row is a requirement of the framework, assessed from the evidence route stated on the row; the entity's own controls have not been registered against the requirements and no population was sampled, so these results are readiness findings for the assessor, not tests of the entity's controls.

APRA notification (2)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
cl-35	APRA notification	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** close call (an assessor decides)	011_data_breach_response_procedure.pdf · `4bc5e0e094ad…` 208_incident_post_mortem_q3_2025.pdf · `72971ff13676…` 118_incident_post_mortem_q2_2026.pdf · `ee3caab338c2…` *"Summary of results Security incident INC-2026-0142 — business email compromise, severity 2 Time to detect / contain 41 min / 2h 10m Customer impact None confirmed Notifications APRA CPS 234 within 72h; OAIC assessment — not eligible 3."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Candidate evidence — assessor review	Provide evidence to enable an evidence-led result.
cl-36	APRA notification	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** not shown by the documents cited	011_data_breach_response_procedure.pdf · `4bc5e0e094ad…` 010_incident_response_plan.pdf · `42ae39730590…` *"Scope This document applies to all employees, contractors, temporary staff and third parties acting for Southern Mutual Bank, and to all information assets, systems and environments it operates or operates on its behalf — on-premise, cloud (AWS/Azure), SaaS and outsourced services."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Candidate evidence — assessor review	Provide evidence to enable an evidence-led result.

*How to read this table: one row per control, grouped under the control area named in the heading above each block. **Name / area** is the control's own name where this framework's catalogue gives one, and the control area otherwise — some catalogues name their controls only by identifier, and repeating the identifier or the area heading beside it would tell a reader nothing they do not already have on the line.*

Requirement text for the controls reported above.

cl-35

An APRA -regulated entity must notify APRA as soon as possible and , in any case, no later than 72 hours , after becoming aware of an information security incident that: (a) materially affect ed, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders , beneficiaries or other customers ; or (b) has been notified to other regulators, either in Australia or other jurisdictions.14

cl-36

An APRA -regulated entity must notify APRA as soon as possible and , in any case, no later than 10 business days , after it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner .

9a. Evidence register

Each evidence item with the control it supports and its provenance — the same evidence assessed in the ISM/IRAP assessment, crosswalked to this framework. Each evidence item carries its SHA-256 integrity hash below — a tamper-evident chain of custody over the cited artefacts.

#	Control	Cited document	Provenance	Integrity (SHA-256)
1	cl-6	020_vendor_security_assessment_standard.pdf	Uploaded evidence	0cb5dc4bae48d77f4f42f23d5df9b8b917b55972359ebf8d4cb54a6931c4b79c
2	cl-6	116_vendor_assurance_evidence_soc_2_summary_microsoft_q2_2026.pdf	Uploaded evidence	cc7f4de7a50d8656f4336a9392093d64363f916e2bd1b9b01ec757be50284b5d
3	cl-6	206_vendor_assurance_evidence_soc_2_summary_microsoft_q3_2025.pdf	Uploaded evidence	dbd97aab0e7b324a230bc4c3db682cdbcf0861beb43e82884aed223cd246be1a
4	cl-14	029_security_governance_committee_charter.pdf	Uploaded evidence	e59df87042d8710787d77651b1ea20bd7fa9e9a2d76f733608670d68b91b4a35
5	cl-16	020_vendor_security_assessment_standard.pdf	Uploaded evidence	0cb5dc4bae48d77f4f42f23d5df9b8b917b55972359ebf8d4cb54a6931c4b79c
6	cl-16	116_vendor_assurance_evidence_soc_2_summary_microsoft_q2_2026.pdf	Uploaded evidence	cc7f4de7a50d8656f4336a9392093d64363f916e2bd1b9b01ec757be50284b5d
7	cl-16	206_vendor_assurance_evidence_soc_2_summary_microsoft_q3_2025.pdf	Uploaded evidence	dbd97aab0e7b324a230bc4c3db682cdbcf0861beb43e82884aed223cd246be1a
8	cl-17	104_vulnerability_scan_report_core_banking_temenos_t24_q2_2026.pdf	Uploaded evidence	57d272bb1f0ca21a99285efb37ed16d6b1176c057d8a4802072a3e6d81ccc75f
9	cl-17	112_patch_compliance_report_core_banking_temenos_t24_q2_2026.pdf	Uploaded evidence	159ccb7ae03586d8751c6cef5334f856b107f8844678e78d8733e94602e44a2d
10	cl-19	002_access_control_policy.pdf	Uploaded evidence	b0d7557047740e19743dc4450ec30df6db69ae4d366742e28bbc043e912b8189
11	cl-19	019_third_party_risk_management_policy.pdf	Uploaded evidence	dc41ed8ba096218cf792bf099aa22c2ea9b17be6d8f283474a95a004fccbc2fb
12	cl-19	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e980b10188f726e4e250bec6d8a40da3e43
13	cl-20	023_data_classification_handling_standard.pdf	Uploaded evidence	056d78ec3f060b14840e6d03e256abafd58ff5517ea0602993989da373920172
14	cl-23	208_incident_post_mortem_q3_2025.pdf	Uploaded evidence	72971ff13676a070d519006e11981d4f404f7a93f71ad11bd0b16108e8cc9b51
15	cl-23	118_incident_post_mortem_q2_2026.pdf	Uploaded evidence	ee3caab338c2fe87bc753c91d76209313be05224d77f63843081421874d3084b
16	cl-24	208_incident_post_mortem_q3_2025.pdf	Uploaded evidence	72971ff13676a070d519006e11981d4f404f7a93f71ad11bd0b16108e8cc9b51
17	cl-24	118_incident_post_mortem_q2_2026.pdf	Uploaded evidence	ee3caab338c2fe87bc753c91d76209313be05224d77f63843081421874d3084b
18	cl-25	011_data_breach_response_procedure.pdf	Uploaded evidence	4bc5e0e094add1c8bd11f714951f91afccb8ae920e28b586ccbfc49b921601ba
19	cl-25	010_incident_response_plan.pdf	Uploaded evidence	42ae3973059050231da613b651b6b2ce0ac19f4ae2d69bb4d8a17abdbaae5d6b
20	cl-25	008_logging_monitoring_policy.pdf	Uploaded evidence	808a97e670d8c146b60deffd1db23c48631586d78316946224c5e30f191f36ae
21	cl-26	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	4027f4cd46d73e3ce32e965c8a49a215e5e432bf08703655d804c28af27dc3b2
22	cl-26	010_incident_response_plan.pdf	Uploaded evidence	42ae3973059050231da613b651b6b2ce0ac19f4ae2d69bb4d8a17abdbaae5d6b
23	cl-26	013_disaster_recovery_plan.pdf	Uploaded evidence	43e28b398d1d5644d3719a74fee67c20af34499386b572d0f34c6bf01675ad6e
24	cl-26	014_backup_restoration_standard.pdf	Uploaded evidence	9342ac709c3737c18af8f9c2eaa8f558e448604bc0944a018c5f682982da69b9
25	cl-27	052_audit_findings_risk_treatment_register.pdf	Uploaded evidence	5cc25603c344aeeebeaab3ca11ecd9f9a02128575ef1e8e5c8536da2d21cd56f
26	cl-28	020_vendor_security_assessment_standard.pdf	Uploaded evidence	0cb5dc4bae48d77f4f42f23d5df9b8b917b55972359ebf8d4cb54a6931c4b79c
27	cl-28	116_vendor_assurance_evidence_soc_2_summary_microsoft_q2_2026.pdf	Uploaded evidence	cc7f4de7a50d8656f4336a9392093d64363f916e2bd1b9b01ec757be50284b5d
28	cl-28	206_vendor_assurance_evidence_soc_2_summary_microsoft_q3_2025.pdf	Uploaded evidence	dbd97aab0e7b324a230bc4c3db682cdbcf0861beb43e82884aed223cd246be1a
29	cl-32	052_audit_findings_risk_treatment_register.pdf	Uploaded evidence	5cc25603c344aeeebeaab3ca11ecd9f9a02128575ef1e8e5c8536da2d21cd56f

#	Control	Cited document	Provenance	Integrity (SHA-256)
30	cl-33	052_audit_findings_risk_treatment_register.pdf	Uploaded evidence	`5cc25603c344aeeebeaab3ca11ecd9f9 a02128575ef1e8e5c8536da2d21cd56f`
31	cl-34	020_vendor_security_assessment_standard.pdf	Uploaded evidence	`0cb5dc4bae48d77f4f42f23d5df9b8b9 17b55972359ebf8d4cb54a6931c4b79c`
32	cl-35	011_data_breach_response_procedure.pdf	Uploaded evidence	`4bc5e0e094add1c8bd11f714951f91af ccb8ae920e28b586ccbfc49b921601ba`
33	cl-35	208_incident_post_mortem_q3_2025.pdf	Uploaded evidence	`72971ff13676a070d519006e11981d4f 404f7a93f71ad11bd0b16108e8cc9b51`
34	cl-35	118_incident_post_mortem_q2_2026.pdf	Uploaded evidence	`ee3caab338c2fe87bc753c91d7620931 3be05224d77f638430814218 74d3084b`
35	cl-36	011_data_breach_response_procedure.pdf	Uploaded evidence	`4bc5e0e094add1c8bd11f714951f91af ccb8ae920e28b586ccbfc49b921601ba`
36	cl-36	010_incident_response_plan.pdf	Uploaded evidence	`42ae3973059050231da613b651b6b2ce 0ac19f4ae2d69bb4d8a17abdbaae5d6b`

How the counts relate. This register has one row per control–document citation: 36 citations of 19 distinct documents across 17 controls. A document cited against several controls appears once for each. The evidence freshness statement counts every item in the submission, cited or not, so its total differs from both.

9b. Evidence integrity and hash manifest

Each evidence item carries a SHA-256 integrity hash and the assessment baseline is hash-stamped, so the control record is tamper-evident. The manifest hash below binds the framework, the assessed entity and the generation time, every one of the 26 assessed controls with its result, the 19 cited evidence documents by name and the 19 evidence SHA-256 hashes recorded for them.

Distinct evidence artefacts	19
Controls with cited evidence	17
Artefacts carrying a SHA-256 hash	19 of 19
Manifest hash (SHA-256)	f0c6d563bca3d06049848c4b47a8b74a47a95491e04debf65b3284d65d13b48f

9c. Cross-framework control mapping

Each evidence signal maps across frameworks, so a single assessment run is ASSESSED against this framework and the others below simultaneously — collect once, report everywhere. Mapping is not a verdict: each framework's result is its own, and appears in that framework's control assessment. **In this engagement no live signal reached any control**, so this describes what the platform can collect once a source is connected. It is not evidence in this report.

Evidence signal	This framework	Also evidences (other frameworks)
mfa	cl-21	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, CyberSentien HITRUST CSF Readiness Assessment, ISM / IRAP SAR, ISO/IEC 27001:2022
conditional access	cl-21	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0
privileged roles	cl-21	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0
guest accounts	cl-21	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, PCI DSS v4.0.1
dormant accounts	cl-21	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0
network segmentation	cl-21	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, PCI DSS v4.0.1
firewall policy	cl-21	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, PCI DSS v4.0.1

Evidence signal	This framework	Also evidences (other frameworks)
transport encryption	cl-21	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, PCI DSS v4.0.1
network exposure	cl-21	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, PCI DSS v4.0.1
central logging	cl-23	APRA CPS 230 (Operational Risk), Breach Reporting (OAIC NDB / CPS 234), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, EU AI Act (Regulation 2024/1689)
os patching	cl-21	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0
vulnerability exposure	cl-27	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, EU AI Act (Regulation 2024/1689), ISM / IRAP SAR, ISO/IEC 27001:2022
dlp	cl-21	Breach Reporting (OAIC NDB / CPS 234), CIS Controls v8, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST SP 800-53 Rev 5, NIST CSF 2.0
retention	cl-21	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, Australian Early Childhood (ECEC — National Law, privacy & child safety), Fraud & AML (AUSTRAC AML/CTF), ISM / IRAP SAR, ISO/IEC 27001:2022
sensitivity labels	cl-20	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST SP 800-53 Rev 5, NIST CSF 2.0
security defaults	cl-21	CIS Controls v8, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, PCI DSS v4.0.1
application control	cl-21	CIS Controls v8, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, PCI DSS v4.0.1
device inventory	cl-20	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, Australian Early Childhood (ECEC — National Law, privacy & child safety), ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022
device encryption	cl-21	Australian Early Childhood (ECEC — National Law, privacy & child safety), ISM / IRAP SAR, ISO/IEC 27001:2022, Australian Schools (cyber, privacy & child safety)
incident response	cl-23	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, Australian Early Childhood (ECEC — National Law, privacy & child safety), ISM / IRAP SAR, ISO/IEC 27001:2022, NIST SP 800-53 Rev 5
access governance	cl-21	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, Fraud & AML (AUSTRAC AML/CTF), ISM / IRAP SAR, ISO/IEC 27001:2022, NIST SP 800-53 Rev 5
email security	cl-21	Breach Reporting (OAIC NDB / CPS 234), CIS Controls v8, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0
external collaboration	cl-21	ISO/IEC 27001:2022, SOC 1 (ISAE 3402 / SSAE 18), SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
data sharing	cl-21	ISO/IEC 27001:2022, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
identity groups	cl-21	CIS Controls v8, ISO/IEC 27001:2022, NIST CSF 2.0, PCI DSS v4.0.1, SOC 1 (ISAE 3402 / SSAE 18), SOC 2 (Trust Services Criteria)
domain verification	cl-21	ISM / IRAP SAR, ISO/IEC 27001:2022, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
endpoint protection	cl-21	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, CyberSentien HITRUST CSF Readiness Assessment, ISM / IRAP SAR, ISO/IEC 27001:2022

Evidence signal	This framework	Also evidences (other frameworks)
siem logging	cl-23	Breach Reporting (OAIC NDB / CPS 234), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, EU AI Act (Regulation 2024/1689), Fraud & AML (AUSTRAC AML/CTF)
ai data governance	cl-21	CyberSentien AI Governance Assurance, AU AI Ethics Principles, AU Gov — Responsible Use of AI, EU AI Act (Regulation 2024/1689), ISO/IEC 42001:2023 (AI Management System), NIST AI RMF 1.0
ai access control	cl-21	CyberSentien AI Governance Assurance, EU AI Act (Regulation 2024/1689), ISO/IEC 42001:2023 (AI Management System), NIST AI RMF 1.0, NSW GenAI Guidance
mfa enforced all users	cl-21	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
mfa enforced privileged	cl-21	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
legacy auth blocked	cl-21	ISO/IEC 27001:2022, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
global admin count bounded	cl-21	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
inactive unprivileged disabled	cl-21	ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
device compliance complete	cl-21	ISO/IEC 27001:2022, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
edr onboarding complete	cl-23	ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
high severity alerts triaged	cl-23	ISO/IEC 27001:2022, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
email dmarc reject	cl-21	ISM / IRAP SAR, ISO/IEC 27001:2022
email spf hard fail	cl-21	ISM / IRAP SAR, ISO/IEC 27001:2022
email dkim signing	cl-21	ISM / IRAP SAR, ISO/IEC 27001:2022
email attachment filtering	cl-21	ISM / IRAP SAR, ISO/IEC 27001:2022, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
sharepoint anonymous sharing disabled	cl-21	ISO/IEC 27001:2022, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
aws root mfa	cl-21	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
aws root access keys absent	cl-21	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
aws console mfa	cl-21	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
aws inactive credentials disabled	cl-21	ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)

10. Evidence freshness statement

This report was generated using evidence with document/upload dates up to 2026-11-10T05:36:44+00:00. The earliest evidence date is not recorded, so the age of the oldest item relied upon cannot be stated. No live-connector collection time was recorded. Uploaded documents were assessed on document date, upload date, version and stated review date. Evidence older than the defined freshness threshold is marked stale and is not treated as current assurance unless confirmed by the assessor.

Report classification: manual review required · Freshness confidence: insufficient for current assurance · Control index: not recorded. (The framework edition this report is assessed against is stated on the cover.)

Evidence freshness: 0 fresh · 0 aging · 0 stale · 0 expired · 0 missing · 76 manual-review (of 76 items).

The 76 items counted above are every dated evidence item recorded for this scope. The evidence register lists 19 distinct documents cited against this framework's controls. The two populations are different — a scope may hold evidence no control in this framework cites, and a document may be cited many times — so the counts are not expected to agree.

11. AI assurance statement

Verdicts are assessor-owned. AI assists retrieval, verification and drafting, and for this framework an AI review may credit a control: only where it confirmed the evidence at the threshold its accuracy test set, and always with the passage it rests on. Every credit REQUIRES assessor confirmation before the report is issued.

Logic mode in force: evidence-led verdicts with the AI review on for this framework. Retrieval proposes candidate links; the AI review credits a control only where it is sure, and everything else is shown for assessor confirmation.

AI components: Evidence-to-control matching (assistive retrieval, sovereign semantic retrieval); Local-LLM verification & grounded citation (assistive verification, sovereign verification model); Assessor observation drafting (assistive drafting, sovereign verification model); Ask CyberSentien (framework lens) (assistive advisory generation over deterministic grounding, sovereign verification model); AI review of uploaded evidence (credits a control only at its tested threshold).

Sovereignty: in this sample the AI review ran on a rented GPU over the fictional documents only; every other step ran inside this deployment. For a client the AI review runs on hardware the client operates or on a sovereign GPU the client arranges. The exact model identifiers and versions used for this run, and the accuracy test results behind the credits, are disclosed to the client and their auditor on request.

Accuracy: AI credits are shown only for frameworks whose AI review has passed an independent accuracy test. For CPS 234 that test result is: at least 95% correct (9 wrong in 319 tested). Each AI credit in this report shows the passage it rests on; every other finding is shown for assessor review.

For this report, an assessor has recorded their own statement, so the confirmation described above has been given and is on the record in the assessor statement.

12. APRA CPS 234 (Information Security) readiness conclusion

Of 26 controls, 0 were assessed from evidence (so no implementation rate can be stated). Outstanding: 9 requiring assessor review — no signal or uploaded evidence; 13 candidate evidence — assessor review; 4 insufficient evidence. This is a CyberSentien readiness assessment aligned to APRA CPS 234 / CPG 234. It supports the entity's own assurance and Board reporting; it is not an independent assurance engagement and does NOT constitute APRA approval.

This is a CyberSentien continuous-assurance / readiness assessment. It is not a certification or attestation decision, which requires an accredited/registered assessor or CPA firm to review the evidence, complete issuance governance, and sign off.

13. Risk ratings and remediation plan

Each control not yet shown as implemented is rated by the size of the readiness gap. **High**: the evidence shows the control absent or not operating, or its operation cannot be observed. **Medium**: the evidence supports the control only in part, is out of date, does not establish it, or none is on file. **Low**: candidate evidence is on file and awaits the assessor's confirmation. A rating describes the gap in the evidence, not a finding that the control has failed. Target dates run from the date of this readiness assessment: 30 days for High, 60 for Medium, 90 for Low.

0 High · 13 Medium · 13 Low — 26 open controls in all.

Control	Risk	Why rated	Action	Suggested owner (role)	Target date
cl-10	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Engineering lead	2027-01-08
cl-13	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Incident and continuity lead	2027-01-08
cl-15	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Information security manager	2027-01-08
cl-18	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Information security manager	2027-01-08

Control	Risk	Why rated	Action	Suggested owner (role)	Target date
cl-21	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Information security manager	2027-01-08
cl-22	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Information security manager	2027-01-08
cl-23	**Medium**	The evidence supplied does not establish the control	Supply operating records that show the control working during the period	Incident and continuity lead	2027-01-08
cl-24	**Medium**	The evidence supplied does not establish the control	Supply operating records that show the control working during the period	Incident and continuity lead	2027-01-08
cl-27	**Medium**	The evidence supplied does not establish the control	Supply operating records that show the control working during the period	Engineering lead	2027-01-08
cl-29	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Engineering lead	2027-01-08
cl-30	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Engineering lead	2027-01-08
cl-31	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Engineering lead	2027-01-08
cl-33	**Medium**	The evidence supplied does not establish the control	Supply operating records that show the control working during the period	Information security manager	2027-01-08
cl-6	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Engineering lead	2027-02-07
cl-14	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Incident and continuity lead	2027-02-07
cl-16	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
cl-17	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
cl-19	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
cl-20	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
cl-25	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Incident and continuity lead	2027-02-07
cl-26	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Incident and continuity lead	2027-02-07
cl-28	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Engineering lead	2027-02-07
cl-32	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
cl-34	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
cl-35	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07

Control	Risk	Why rated	Action	Suggested owner (role)	Target date
cl-36	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07

How to read this table: the owner is a suggested role taken from the control's own area; name the accountable person for each action before work starts. An action closes when its evidence is re-submitted and the control is re-assessed.

Assessor statement

Authored by the assessor (Alex Morgan (fictional), Lead assessor) on 2026-11-10 — the assessor's own words, presented verbatim and separately from engine-derived findings.

I have reviewed the results in this readiness assessment against the evidence cited for each control and accept them as the basis of this report. Controls shown as candidate evidence for assessor review remain open, and are rated and dated in the risk ratings and remediation plan. The organisation, people and evidence in this report are fictional.

C. Appendix — CISSP-domain governance registers

The continuous-assurance governance registers this platform maintains, grouped by CISSP domain. Each register reports its own live rollup; a register with no data is shown honestly as 'No data recorded' — nothing is fabricated. These complement the control-by-control assessment above with the operating-model registers a mature programme is expected to keep. **A register reading 'No data recorded' means nothing has been entered in it on the platform.** It is not a statement that the entity has no such records: documents supplied as evidence (an incident post-mortem, a vendor assurance report) are assessed in the control assessment and listed in the evidence register, and do not populate these registers.

C.1 CISSP D1 — Security & Risk Management

Register	Headline	Detail
Enterprise risk register	0 open risks	*No data recorded (no risks in the register).*
Obligation corpus	0 active obligations	*No data recorded (no obligations captured).*
Third-party register (TPRM)	0 providers	*No data recorded (no third parties registered). 2 third-party assurance records supplied as evidence are assessed in the control assessment and listed in the evidence register (for example 116_vendor_assurance_evidence_soc_2_summary_microsoft_q2_2026.pdf).*

C.2 CISSP D2 — Asset Security

Register	Headline	Detail
Asset & data governance	0 assets governed	*No data recorded (no assets governed).*

C.3 CISSP D3 — Security Architecture & Engineering

Register	Headline	Detail
Boundary threat model (STRIDE)	threat model to be agreed with the assessor	*No data recorded (no threat model for this scope).*
Secure-design principles	0 of 6 principles met	*No data recorded (no evidence for any principle).*
Shared-responsibility matrix	0 controls mapped	*No data recorded (no responsibility matrix for this submission).*

C.4 CISSP D4 — Communication & Network Security

Register	Headline	Detail
Attack-surface exposure	0 exposures tracked	*No data recorded (no exposures tracked).*

C.5 CISSP D5 — Identity & Access Management

Register	Headline	Detail
Privileged-access assurance (PAM)	no PAM signal	*No data recorded (no privileged-access records collected).*

C.6 CISSP D6 — Security Assessment & Testing

Register	Headline	Detail
Assessment plans	0 plan(s)	*No data recorded (no assessment plan captured).*
Sampling methodology	0 sampling plan(s)	*No data recorded (no sampling plans — manual controls unsampled). Every test in this report is a documentary review; no population was sampled.*
Control register	0 governed controls	*No data recorded (no first-class control objects). Each row of the control assessment is a framework requirement, not one of the entity's own controls; the entity's controls are recorded here before testing.*
Finding register	0 finding(s)	*No data recorded (no findings raised).*

C.7 CISSP D7 — Security Operations

Register	Headline	Detail
Incident register	0 open of 0	*No data recorded (no incidents logged). 2 incident records supplied as evidence are assessed in the control assessment and listed in the evidence register (for example 118_incident_post_mortem_q2_2026.pdf).*
Investigation register	0 open of 0	*No data recorded (no investigation cases opened).*
DR & recovery exercises	0 exercises run	*No data recorded (no DR exercises run).*
Business impact analysis (BIA)	0 critical operations	*No data recorded (no operations analysed).*

C.8 CISSP D8 — Software Development Security

Register	Headline	Detail
Secure SDLC gates	0 projects tracked	*No data recorded (no SDLC projects tracked).*
SBOM & VEX (supply chain)	0 components	*No data recorded (no SBOM ingested).*

How to read this table: one row per governance register, grouped by CISSP domain. The headline is the register's own live rollup; a register with no data is shown as 'No data recorded' in grey — the appendix never asserts a figure a register does not hold (no false green).

E. Appendix — controls excluded from assessment

These catalogued rows are not obligations this engine assesses, so they carry no result and are outside every count in this report. They are listed in full so the published catalogue can be reconciled against what was assessed: 10 excluded, 26 assessed, 36 catalogued.

Control	Title	Why it is not assessed	Where the obligation now sits
cl-1	Application & interpretation	The instrument stating when it commences — not an obligation on the entity	—
cl-5	Application & interpretation	The instrument stating when it commences — not an obligation on the entity	—
cl-12	Application & interpretation	Definitions — not an obligation on the entity	—
cl-7	Application & interpretation	Definitions — not an obligation on the entity	—
cl-8	Application & interpretation	Definitions — not an obligation on the entity	—
cl-11	Application & interpretation	The instrument stating how it is to be read — not an obligation on the entity	—
cl-9	Application & interpretation	The instrument stating how it is to be read — not an obligation on the entity	—
cl-2	Application & interpretation	The instrument stating what it applies to — not an obligation on the entity	—
cl-3	Application & interpretation	The instrument stating what it applies to — not an obligation on the entity	—
cl-4	Application & interpretation	The instrument stating what it applies to — not an obligation on the entity	—

How to read this table: each row is a clause of the standard that sets out how the standard applies or is read, rather than a requirement on the entity, so it is not rated.

F. Appendix — evidence to collect next

Each control the AI review held back, with the evidence that would show it. The evidence named is the engine catalogue's own expected evidence for the control, operating records first. A close call already has candidate evidence on file: an assessor reviews it first, and collects more only if it falls short.

Control	Title	Why it is listed	Evidence to collect
cl-14	Roles and responsibilities	Close call: an assessor reviews the cited document first	An approval record; a governance record (minutes or a decision record)
cl-16	Information security capability	Close call: an assessor reviews the cited document first	Incident records; an extract from the relevant register; supplier assurance reports
cl-17	Information security capability	Close call: an assessor reviews the cited document first	A vulnerability scan report; a signed review record; an extract from the relevant register
cl-19	Policy framework	Close call: an assessor reviews the cited document first	An approval record; an extract from the relevant register; supplier assurance reports
cl-23	Incident management	Close call: an assessor reviews the cited document first	Incident records; a signed review record; an assessment record
cl-25	Incident management	Close call: an assessor reviews the cited document first	A vulnerability scan report; monitoring records (alerts and their triage); incident records
cl-27	Testing control effectiveness	Close call: an assessor reviews the cited document first	A vulnerability scan report; incident records; a signed review record
cl-32	Internal audit	Close call: an assessor reviews the cited document first	A signed review record; audit records; an assessment record
cl-35	APRA notification	Close call: an assessor reviews the cited document first	Incident records; a governance record (minutes or a decision record); a documented procedure
cl-20	Identification & classification	The documents cited do not show it	Incident records; an assessment record; an extract from the relevant register
cl-24	Incident management	The documents cited do not show it	Incident records; an approved plan
cl-26	Incident management	The documents cited do not show it	A signed review record; an approved plan
cl-28	Testing control effectiveness	The documents cited do not show it	An extract from the relevant register; supplier assurance reports; the relevant contract clauses
cl-33	Internal audit	The documents cited do not show it	Training completion records; audit records; an assessment record
cl-34	Internal audit	The documents cited do not show it	Incident records; audit records; an assessment record
cl-36	APRA notification	The documents cited do not show it	Incident records; an exercise record; an extract from the relevant register
cl-6	Application & interpretation	The documents cited do not show it	An extract from the relevant register; supplier assurance reports; the relevant contract clauses