ISO/IEC 27001:2022 — ISMS Assessment & Certification-Readiness Report

Information Security Management System assessment against ISO/IEC 27001:2022

Organisation / system in scope	Southern Mutual Bank (fictional) / Core banking and customer channels
Framework	ISO/IEC 27001:2022 · ISO/IEC · 2022 (93 Annex A controls + clauses 4-10)
Report type	ISMS assessment — certification readiness
Assessment basis / period	As at 2026-11-09
Controls assessed	116
Evidence-led coverage	8 of 116 reached a verdict from evidence
Evidence reach	107 of 116 controls carry uploaded evidence (0 of those also carry a live signal); 9 carry neither
Report number	CS-SMB-2026-003
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 ISMS assessment / certification-readiness report. It is NOT an ISO certification decision, which requires an accredited certification body to conduct a Stage 1 and Stage 2 audit and issue the certificate. Annex A controls are referenced by identifier and CyberSentien's own short labels — no copyrighted ISO text is reproduced.

Contents

§	Section
—	Document control, governance and issuance
—	Report format and standard alignment
—	How to read the results
—	Executive summary
—	What the engine did
1	Management-system clauses 4-10
2	ISMS scope & boundary
3	Annex A control assessment (by theme)
4	Statement of Applicability
5	Nonconformities (major/minor)
6	Corrective action plan
7	Risk assessment & treatment linkage
8	Internal audit & management review
9	Evidence freshness statement
10	AI assurance statement
11	ISO/IEC 27001:2022 certification readiness conclusion
12	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-2026-003

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: external-issue approval not recorded

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 ISO 27001: at least 95% correct (4 wrong in 185 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: 82 not confirmed by the AI review. Each lists its candidates and the reason.

Report format and standard alignment

Obligation pack / sources	ISO/IEC 27001:2022 · ISO/IEC
Version	2022 (93 Annex A controls + clauses 4-10)
Report format followed	ISMS assessment — certification readiness
Primary source cited	https://www.iso.org/standard/27001
Source access	licensed

This report follows CyberSentien's own reporting structure for ISO/IEC 27001:2022. 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. Sections covered:

1. Management-system clauses 4-10
2. ISMS scope & boundary
3. Annex A control assessment (by theme)
4. Statement of Applicability
5. Nonconformities (major/minor)
6. Corrective action plan
7. Risk assessment & treatment linkage
8. Internal audit & management review

Companion artefacts in this framework's report family: ISMS assessment report, Statement of Applicability, risk assessment register, risk treatment plan, internal audit report, management review pack, nonconformity register, corrective action plan, certification-readiness 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.

Executive summary

0%	0	9
implemented (of evidence-led)	gaps / not met	manual assessment required

Against ISO/IEC 27001:2022, 8 of 116 controls were assessed from evidence (continuous signals and the assessor's uploaded evidence), of which 0 are implemented, 8 partially, and 0 are gaps. 9 controls have no automated signal or uploaded evidence and require assessor review. A further 99 are outstanding: 81 candidate evidence — assessor review; 18 insufficient evidence — assessed, not established. All figures are evidence-led; nothing is asserted as compliant without evidence (no false green).

Priority remediation areas (by adverse-control density): Technological (8).

Executive remediation roadmap — what to fix first

The assessed gaps, sequenced for decision-makers. NOW = controls with failed evidence (active exposure); NEXT = partially evidenced controls (close the gap to full assurance); LATER = controls whose evidence has lapsed or is no longer observable (stale, or visibility lost). Derived deterministically from this report's own adverse findings — the same controls, in the same states, reported throughout this report; owners and dates are assigned by the accountable executive.

Wave	Theme (business terms)	Why it matters	Controls
NEXT	Strengthen Technological	8 controls are partially evidenced — working practice exists but would not fully withstand assurance challenge.	A.8.1, A.8.2, A.8.9, A.8.12, A.8.13 and 3 more

How to read this table: rows are grouped by wave, and within a wave by worst exposure first. Waves sequence the programme: complete every NOW row before NEXT. Each row names the controls its own count refers to.

A further 27 controls are not in this roadmap because nothing in this submission establishes them either way — they are not adverse findings, and are reported as evidence gaps in the control assessment rather than as weaknesses here.

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	116
Controls with a document cited against them	107
Controls the document matcher put forward from the documents, each read by the AI review	107
Confirmed by the AI review and shown as a credit, with the passage it rests on	8
Refused by the AI review: the documents cited do not show the control	72
Close calls the AI review left for an assessor to decide	27
Controls with no document cited, so nothing for the AI review to read	9
The AI review's tested accuracy for ISO 27001	181 of 185 credits right (97.8%) in an independent test on fictional evidence

1. Management-system clauses 4-10

The controls this assessment holds under "Management system (clauses 4–10)", 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.

Management system (clauses 4–10) (23)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
4.1	Understanding the organisation and its context	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.
4.2	Needs and expectations of interested parties	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.
4.3	Determining the scope of the ISMS	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.
4.4	Information security management system	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	001_information_security_policy.pdf · `19b799381535…` 046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 032_operational_resilience_policy_cps_230.pdf · `4027f4cd46d7…` *+ 1 more cited (see the evidence register)* *“Control objectives: ■ Establish clear accountability, risk appetite and oversight for information security and operational risk.”* 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
5.1	Leadership and commitment	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	001_information_security_policy.pdf · `19b799381535…` 032_operational_resilience_policy_cps_230.pdf · `4027f4cd46d7…` 025_network_security_policy.pdf · `99f3533716db…` *+ 2 more cited (see the evidence register)* *"Purpose and control objectives This policy establishes the requirements, accountabilities and control objectives for information security policy across Southern Mutual Bank ("the Bank")."* 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.
5.2	Policy	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)	001_information_security_policy.pdf · `19b799381535…` 046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 032_operational_resilience_policy_cps_230.pdf · `4027f4cd46d7…` *+ 1 more cited (see the evidence register)* *"Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available."* 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.
5.3	Organisational roles, responsibilities and authorities	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)	001_information_security_policy.pdf · `19b799381535…` 046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 032_operational_resilience_policy_cps_230.pdf · `4027f4cd46d7…` *+ 1 more cited (see the evidence register)* *"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.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
6.1	Actions to address risks and opportunities	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	046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 011_data_breach_response_procedure.pdf · `4bc5e0e094ad…` *+ 1 more cited (see the evidence register)* *"Southern Mutual Bank — Internal Use Only · UNCONTROLLED WHEN PRINTED · SYNTHETIC TEST DOCUMENT Page 8 4.9.1 Risks within this control area shall be identified, assessed (likelihood × impact), treated and recorded in the enterprise risk register with an accountable owner."* 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.
6.2	Information security objectives and planning	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	013_disaster_recovery_plan.pdf · `43e28b398d1d…` 010_incident_response_plan.pdf · `42ae39730590…` *"Purpose and control objectives This plan establishes the requirements, accountabilities and control objectives for disaster recovery plan across Southern Mutual Bank ("the Bank")."* 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.
6.3	Planning of changes	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	010_incident_response_plan.pdf · `42ae39730590…` 013_disaster_recovery_plan.pdf · `43e28b398d1d…` *"In scope Out of scope / exclusions Production, management and DR environments; Core banking platform; identity, endpoint, network and data 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.
7.1	Resources	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
7.2	Competence	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)	128_security_awareness_training_completion_report_q2_2026.pdf · `15697abedbea…` 218_security_awareness_training_completion_report_q3_2025.pdf · `440dd0e6d2e4…` 209_phishing_simulation_results_q3_2025.pdf · `517564d4904a…` *+ 1 more cited (see the evidence register)* *"Scope and method This report records the results of security awareness training completion report for Southern Mutual Bank over the reporting period."* 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.
7.3	Awareness	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)	041_physical_environmental_security_policy.pdf · `d0fa967acaaf…` 016_patch_management_standard.pdf · `7d5c195985fd…` 043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` *+ 2 more cited (see the evidence register)* *"Scope and method This report records the results of security awareness training completion report for Southern Mutual Bank over the reporting period."* 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.
7.4	Communication	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	046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 011_data_breach_response_procedure.pdf · `4bc5e0e094ad…` *+ 1 more cited (see the evidence register)* *"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.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
7.5	Documented information	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)	001_information_security_policy.pdf · `19b799381535…` 046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 032_operational_resilience_policy_cps_230.pdf · `4027f4cd46d7…` *+ 1 more cited (see the evidence register)* *"4.6.2 This document shall be reviewed at least annually and after any material change to the business, technology, regulatory or threat environment, with version control maintained."* 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.
8.1	Operational planning and control	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)	046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 047_personal_information_handling_procedure.pdf · `dc109a6f6de6…` 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.	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
8.2	Information security risk assessment	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	037_security_awareness_training_policy.pdf · `3da7a066b10e`… 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.	Candidate evidence — assessor review	Provide evidence to enable an evidence-led result.
8.3	Information security risk treatment	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	046_records_management_data_handling_procedure.pdf · `291c9ae746a6`… 043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183`… 011_data_breach_response_procedure.pdf · `4bc5e0e094ad`… *+ 1 more cited (see the evidence register)* *"4.7.2 Residual risk exceeding the approved risk appetite shall be escalated with a treatment plan and target date."* 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.
9.1	Monitoring, measurement, analysis and evaluation	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)	008_logging_monitoring_policy.pdf · `808a97e670d8`… 1224_application_control_event_log_extract_workstations_q2_2026.pdf · `d8c9185aed67`… 117_soc_monitoring_report_q2_2026.pdf · `06ca0cc7ca28`… *+ 1 more cited (see the evidence register)* *"Scope and method This report records the results of soc monitoring report for Southern Mutual Bank over the reporting period."* 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
9.2	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	001_information_security_policy.pdf · `19b799381535…` 032_operational_resilience_policy_cps_230.pdf · `4027f4cd46d7…` 025_network_security_policy.pdf · `99f3533716db…` *+ 2 more cited (see the evidence register)* *"4.1.2 The three-lines-of-defence model shall be applied: business ownership, risk/compliance oversight, and independent internal audit."* 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.
9.3	Management review	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	010_incident_response_plan.pdf · `42ae39730590…` 013_disaster_recovery_plan.pdf · `43e28b398d1d…` *"4.3.3 A post-incident review shall be conducted for all P1/P2 incidents and remediation 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.
10.1	Continual improvement	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.
10.2	Nonconformity and corrective action	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	046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 011_data_breach_response_procedure.pdf · `4bc5e0e094ad…` *+ 1 more cited (see the evidence register)* *"4.1.2 An on-call incident commander shall be assignable 24x7 with documented escalation paths and contacts."* 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.*

1a. Control requirements (resolved)

The assessed controls with their requirement text, for the 23 controls not reported under a theme section above. Organisation-defined parameters are resolved to the baseline value where set, or shown as the precise descriptor (e.g. [organization-defined frequency]) where the baseline leaves them to the organisation.

Management system (clauses 4–10)

4.1 — Understanding the organisation and its context

Determine external and internal issues relevant to the ISMS and its intended outcomes; context analysis, SWOT/PESTLE, ISMS purpose.

4.2 — Needs and expectations of interested parties

Identify interested parties relevant to the ISMS and their information security requirements, including legal, regulatory and contractual obligations.

4.3 — Determining the scope of the ISMS

Determine and document the boundaries and applicability of the ISMS; scope statement covering interfaces and dependencies.

4.4 — Information security management system

Establish, implement, maintain and continually improve the ISMS and its processes in accordance with the standard.

5.1 — Leadership and commitment

Top management demonstrates leadership and commitment to the ISMS; policy and objectives set, resources provided, effectiveness promoted.

5.2 — Policy

Top management establishes an information security policy appropriate to the organisation, communicated and available as documented information.

5.3 — Organisational roles, responsibilities and authorities

Assign and communicate responsibilities and authorities for roles relevant to information security.

6.1 — Actions to address risks and opportunities

Plan actions to address ISMS risks and opportunities; information security risk assessment and risk treatment process, Statement of Applicability, risk register.

6.2 — Information security objectives and planning

Establish measurable information security objectives at relevant functions and levels and plan how to achieve them.

6.3 — Planning of changes

Changes to the ISMS are carried out in a planned manner.

7.1 — Resources

Determine and provide the resources needed for the ISMS.

7.2 — Competence

Determine, ensure and evidence the competence of persons doing work affecting information security performance; training records.

7.3 — Awareness

Persons are aware of the information security policy, their contribution and the implications of not conforming; awareness programme.

7.4 — Communication

Determine internal and external communications relevant to the ISMS — what, when, with whom and how.

7.5 — Documented information

Create, update and control the documented information required by the ISMS and the standard; document control, version control, retention.

8.1 — Operational planning and control

Plan, implement and control the processes needed to meet requirements and implement the risk treatment actions; operational control.

8.2 — Information security risk assessment

Perform information security risk assessments at planned intervals and when significant changes occur, retaining documented results.

8.3 — Information security risk treatment

Implement the information security risk treatment plan and retain documented information of the results.

9.1 — Monitoring, measurement, analysis and evaluation

Monitor, measure, analyse and evaluate information security performance and the effectiveness of the ISMS; metrics, KPIs, evaluation results.

9.2 — Internal audit

Conduct internal audits at planned intervals to confirm the ISMS conforms and is effectively implemented; audit programme, internal audit report.

9.3 — Management review

Top management reviews the ISMS at planned intervals for continuing suitability, adequacy and effectiveness; management review minutes/pack.

10.1 — Continual improvement

Continually improve the suitability, adequacy and effectiveness of the ISMS.

10.2 — Nonconformity and corrective action

React to nonconformities, take corrective action, and retain documented information; nonconformity register, corrective action plan, CAPA.

1b. 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.

2. ISMS scope & 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

2a. 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 107 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 with CyberSentien's own short labels; copyrighted standard wording is not reproduced. Verdicts are deterministic and human-owned — the assessor confirms.

3. Annex A control assessment (by theme)

The controls this assessment holds under "Organizational" and "People" and "Physical" and "Technological", 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.

Organizational (37)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
A.5.1	Policies for information security	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)	001_information_security_policy.pdf · `19b799381535…` 046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 032_operational_resilience_policy_cps_230.pdf · `4027f4cd46d7…` *+ 1 more cited (see the evidence register)* *"Control owners maintain procedures and runbooks sufficient for a competent operator to execute the control consistently, and review them after any material change to the business, technology or threat environment."* 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.
A.5.2	Information security 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…` 046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 047_personal_information_handling_procedure.pdf · `dc109a6f6de6…` *+ 2 more cited (see the evidence register)* *"Roles and responsibilities (RACI) Role R A C I Responsibility Chief Information Security Officer ✓ ✓ Owns this document; ensures it is current, resourced and effective."* 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.
A.5.3	Segregation of duties	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	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 041_physical_environmental_security_policy.pdf · `d0fa967acaaf…` 053_security_testing_assurance_procedure.pdf · `62b4dd18699d…` *"Personal devices outside the BYOD programme; non-production sandboxes without Bank data (covered by separate standard)."* 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
A.5.4	Management responsibilities	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	001_information_security_policy.pdf · `19b799381535…` 046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 032_operational_resilience_policy_cps_230.pdf · `4027f4cd46d7…` *+ 1 more cited (see the evidence register)* *"Training, awareness and competency Personnel with responsibilities under this document receive role-based training at onboarding and 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.
A.5.5	Contact with authorities	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…` *"Results Timeline Event / response action Owner Status T+00:50 Forensic image captured Mei-Lin Tan Completed T+02:41 Forensic image captured Priya Sharma Completed T+04:36 Incident declared — severity 2 James O'Connor Completed T+06:15 SIEM alert — anomalous privileged logon David Okafor Completed T+08:50 Regulator notified within timeframe Tom Bauer Completed T+10:12 Forensic image captured Aisha"* 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.
A.5.6	Contact with special interest groups	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	029_security_governance_committee_charter.pdf · `e59df87042d8…` 046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 011_data_breach_response_procedure.pdf · `4bc5e0e094ad…` *+ 2 more cited (see the evidence register)* *"The control is monitored in the SIEM with detections mapped to the relevant threats."* 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
A.5.7	Threat intelligence	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`… *"Purpose This register records the audit findings & risk treatment register maintained by Southern Mutual Bank."* 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.
A.5.8	Information security in project 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	052_audit_findings_risk_treatment_register.pdf · `5cc25603c344`… *"Purpose This register records the audit findings & risk treatment register maintained by Southern Mutual Bank."* 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.
A.5.9	Inventory of information and other associated assets	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	104_vulnerability_scan_report_core_banking_temenos_t24_q2_2026.pdf · `57d272bb1f0c`… 112_patch_compliance_report_core_banking_temenos_t24_q2_2026.pdf · `159ccb7ae035`… 202_patch_compliance_report_core_banking_temenos_t24_q3_2025.pdf · `54433d09b730`… *"Scope and method This report records the results of patch compliance report for Southern Mutual Bank over the reporting period."* 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.
A.5.10	Acceptable use of information and other associated assets	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`… 1228_multi_factor_authentication_configuration_export_entra_id_tenant.pdf · `dd3b9d2f6e6a`… 1229_privileged_access_configuration_export_pam_platform.pdf · `31e96f8caef6`… *+ 1 more cited (see the evidence register)* *"6.2 Apply classification at creation; enforce handling via DLP and access controls."* 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
A.5.11	Return of assets	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.
A.5.12	Classification of information	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`… *"Purpose and control objectives This standard establishes the requirements, accountabilities and control objectives for data classification & handling standard across Southern Mutual Bank ("the Bank")."* 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.
A.5.13	Labelling of information	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`… *"Purpose and control objectives This standard establishes the requirements, accountabilities and control objectives for data classification & handling standard across Southern Mutual Bank ("the Bank")."* 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.
A.5.14	Information transfer	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	046_records_management_data_handling_procedure.pdf · `291c9ae746a6`… 047_personal_information_handling_procedure.pdf · `dc109a6f6de6`… *"Control objectives: ■ Protect personal information and other sensitive records throughout their lifecycle through documented handling, records management and record retention rules."* 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
A.5.15	Access control	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	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 002_access_control_policy.pdf · `b0d755704774…` 041_physical_environmental_security_policy.pdf · `d0fa967acaaf…` *+ 1 more cited (see the evidence register)* *"This enforces least privilege, accountability and limits the blast radius of compromise."* 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.
A.5.16	Identity 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)	221_endpoint_protection_console_export_payments_switch.pdf · `b7d7ab942d91…` 131_endpoint_protection_console_export_internet_banking.pdf · `e850c4525d85…` 1228_multi_factor_authentication_configuration_export_entra_id_tenant.pdf · `dd3b9d2f6e6a…` *+ 2 more cited (see the evidence register)* *"Privileged access management platform — configuration Setting Value Status Privileged accounts vaulted 218 of 218 privileged accounts under PAM management; credentials rotated every 30 days Compliant Just-in-time privileged access Enforced — privileged access granted for a maximum of 8 hours on approved request Compliant Privileged access requests validated Every request requires a business"* 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
A.5.17	Authentication information	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…` 001_information_security_policy.pdf · `19b799381535…` 032_operational_resilience_policy_cps_230.pdf · `4027f4cd46d7…` *+ 2 more cited (see the evidence register)* *"4.2 Authentication and credentials 4.2.1 Multi-factor authentication (MFA) shall be enforced for all remote, administrative, internet-facing and customer access, using phishing-resistant factors where supported."* 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.
A.5.18	Access rights	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	002_access_control_policy.pdf · `b0d755704774…` 041_physical_environmental_security_policy.pdf · `d0fa967acaaf…` 022_privacy_policy.pdf · `e9579dc88cc5…` *+ 2 more cited (see the evidence register)* *"4.5.2 Recertification campaigns shall require an explicit approve/revoke decision by the accountable manager; non-response defaults to revocation."* 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.
A.5.19	Information security in supplier relationships	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…` *+ 1 more cited (see the evidence register)* *"Scope and method This report records the results of vendor assurance evidence (soc 2 summary) for Southern Mutual Bank over the reporting period."* 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
A.5.20	Addressing information security within supplier agreements	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`… *+ 2 more cited (see the evidence register)* *"4.1.2 Security obligations, right-to-audit, breach-notification and sub-contracting clauses shall be included in material supplier contracts."* 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.
A.5.21	Managing information security in the ICT supply chain	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`… 052_audit_findings_risk_treatment_register.pdf · `5cc25603c344`… 116_vendor_assurance_evidence_soc_2_summary_microsoft_q2_2026.pdf · `cc7f4de7a50d`… *+ 1 more cited (see the evidence register)* *"Scope and method This report records the results of vendor assurance evidence (soc 2 summary) for Southern Mutual Bank over the reporting period."* 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
A.5.22	Monitoring, review and change management of supplier services	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`… 008_logging_monitoring_policy.pdf · `808a97e670d8`… 116_vendor_assurance_evidence_soc_2_summary_microsoft_q2_2026.pdf · `cc7f4de7a50d`… *+ 2 more cited (see the evidence register)* *"Results Trust services criterion Auditor conclusion Exceptions Our review A1.2 Recovery Operating effectively None Reviewed by Mei-Lin Tan CC6.6 Boundary protection Exception noted — management response accepted 1 — access review sample Reviewed by Priya Sharma CC6.6 Boundary protection Exception noted — remediated 2 — change approval evidence Reviewed by James O'Connor CC7.2 Monitoring Operating"* 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.
A.5.23	Information security for use of cloud services	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	001_information_security_policy.pdf · `19b799381535`… 002_access_control_policy.pdf · `b0d755704774`… 019_third_party_risk_management_policy.pdf · `dc41ed8ba096`… *"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.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
A.5.24	Information security incident management planning and preparation	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…` 022_privacy_policy.pdf · `e9579dc88cc5…` 010_incident_response_plan.pdf · `42ae39730590…` *+ 2 more cited (see the evidence register)* *"Purpose and control objectives This plan establishes the requirements, accountabilities and control objectives for incident response plan across Southern Mutual Bank ("the Bank")."* 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.
A.5.25	Assessment and decision on information security events	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	040_statement_of_applicability.pdf · `692b30be1c54…` 008_logging_monitoring_policy.pdf · `808a97e670d8…` *"4.5 Security operations and response readiness 4.5.1 A 24x7 monitoring capability shall triage alerts within severity-based response times with documented shift handover."* 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.
A.5.26	Response to information security incidents	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…` 022_privacy_policy.pdf · `e9579dc88cc5…` 038_data_retention_disposal_standard.pdf · `7763782c1a38…` *+ 2 more cited (see the evidence register)* *"Scope and method This report records the results of incident post-mortem for Southern Mutual Bank over the reporting period."* 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
A.5.27	Learning from information security incidents	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…` 1222_application_control_allowlist_review_approval_and_sign_off_record_q2_2026.pdf · `c1a53b33df4a…` *+ 1 more cited (see the evidence register)* *"Results Timeline Event / response action Owner Status T+00:39 Lessons learned workshop Mei-Lin Tan Delayed — escalation path unclear T+02:33 Recovery — service restored Priya Sharma Completed T+04:29 Incident declared — severity 2 James O'Connor Completed T+06:13 Incident declared — severity 2 David Okafor Delayed — escalation path unclear T+08:50 SIEM alert — anomalous privileged logon Tom Bauer"* 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.
A.5.28	Collection of evidence	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…` 022_privacy_policy.pdf · `e9579dc88cc5…` 038_data_retention_disposal_standard.pdf · `7763782c1a38…` *+ 2 more cited (see the evidence register)* *"Results Timeline Event / response action Owner Status T+00:50 Forensic image captured Mei-Lin Tan Completed T+02:41 Forensic image captured Priya Sharma Completed T+04:36 Incident declared — severity 2 James O'Connor Completed T+06:15 SIEM alert — anomalous privileged logon David Okafor Completed T+08:50 Regulator notified within timeframe Tom Bauer Completed T+10:12 Forensic image captured Aisha"* 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
A.5.29	Information security during disruption	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…` 022_privacy_policy.pdf · `e9579dc88cc5…` 013_disaster_recovery_plan.pdf · `43e28b398d1d…` *+ 2 more cited (see the evidence register)* *"Control objectives: ■ Maintain delivery of critical operations within tolerance through disruption."* 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.
A.5.30	ICT readiness for business continuity	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…` 013_disaster_recovery_plan.pdf · `43e28b398d1d…` 014_backup_restoration_standard.pdf · `9342ac709c37…` *+ 1 more cited (see the evidence register)* *"Purpose and control objectives This plan establishes the requirements, accountabilities and control objectives for disaster recovery plan across Southern Mutual Bank ("the Bank")."* 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
A.5.31	Legal, statutory, regulatory and contractual requirements	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`… 052_audit_findings_risk_treatment_register.pdf · `5cc25603c344`… 233_network_interconnections_inventory_payments_switch.pdf · `62288f43a45f`… *+ 2 more cited (see the evidence register)* *“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.	Insufficient evidence	Provide evidence to enable an evidence-led result.
A.5.32	Intellectual property rights	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`… *“Southern Mutual Bank — Internal Use Only · UNCONTROLLED WHEN PRINTED · SYNTHETIC TEST DOCUMENT Page 2 4.1.1 An accurate inventory of hardware, software and information assets shall be maintained and reconciled regularly.”* 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
A.5.33	Protection of records	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	1229_privileged_access_configuration_export_pam_platform.pdf · `31e96f8caef6`… 221_endpoint_protection_console_export_payments_switch.pdf · `b7d7ab942d91`… 131_endpoint_protection_console_export_internet_banking.pdf · `e850c4525d85`… *+ 2 more cited (see the evidence register)* *"Privileged access management platform — configuration Setting Value Status Privileged accounts vaulted 218 of 218 privileged accounts under PAM management; credentials rotated every 30 days Compliant Just-in-time privileged access Enforced — privileged access granted for a maximum of 8 hours on approved request Compliant Privileged access requests validated Every request requires a business"* 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.
A.5.34	Privacy and protection of PII	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	046_records_management_data_handling_procedure.pdf · `291c9ae746a6`… 011_data_breach_response_procedure.pdf · `4bc5e0e094ad`… 047_personal_information_handling_procedure.pdf · `dc109a6f6de6`… *+ 2 more cited (see the evidence register)* *"■ Meet obligations under the Privacy Act and the Notifiable Data Breaches scheme."* 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
A.5.35	Independent review of information security	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`… 1222_application_control_allowlist_review_approval_and_sign_off_record_q2_2026.pdf · `c1a53b33df4a`… 1239_trusted_macro_vetting_approval_and_sign_off_record_q3_2026.pdf · `cc7cdf8ff590`… *+ 1 more cited (see the evidence register)* *“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 Compensati ng 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.
A.5.36	Compliance with policies, rules and standards for information security	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`… 1222_application_control_allowlist_review_approval_and_sign_off_record_q2_2026.pdf · `c1a53b33df4a`… 1239_trusted_macro_vetting_approval_and_sign_off_record_q3_2026.pdf · `cc7cdf8ff590`… *+ 1 more cited (see the evidence register)* *“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.	Insufficient evidence	Provide evidence to enable an evidence-led result.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
A.5.37	Documented operating procedures	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)	046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 011_data_breach_response_procedure.pdf · `4bc5e0e094ad…` *+ 1 more cited (see the evidence register)* *"Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available."* 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.*

People (8)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
A.6.1	Screening	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	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 041_physical_environmental_security_policy.pdf · `d0fa967acaaf…` 052_audit_findings_risk_treatment_register.pdf · `5cc25603c344…` *"• Ensure personnel security: pre-employment personnel screening, background checks and security clearances proportionate to role, and controlled termination of employment."* 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
A.6.2	Terms and conditions of employment	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	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 041_physical_environmental_security_policy.pdf · `d0fa967acaaf…` *"4.4 Terms of employment, conduct and termination 4.4.1 Employment contracts and contractor agreements shall include confidentiality, acceptable-use and security responsibilities that survive termination of employment."* 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.
A.6.3	Information security awareness, education and training	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)	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 041_physical_environmental_security_policy.pdf · `d0fa967acaaf…` 128_security_awareness_training_completion_report_q2_2026.pdf · `15697abedbea…` *+ 2 more cited (see the evidence register)* *"Summary of results Security awareness training completion 97.2% (target 98%) Personnel overdue 61 — escalated to people leaders Role-based training — privileged users 100% New starters trained within 30 days 99% Gateway administrators formally trained 14 of 14 — operation and management of gateways 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
A.6.4	Disciplinary process	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	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 041_physical_environmental_security_policy.pdf · `d0fa967acaaf…` 016_patch_management_standard.pdf · `7d5c195985fd…` *"Wilful or negligent breaches may result in disciplinary action up to termination."* 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.
A.6.5	Responsibilities after termination or change of employment	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	001_information_security_policy.pdf · `19b799381535…` 046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 032_operational_resilience_policy_cps_230.pdf · `4027f4cd46d7…` *+ 1 more cited (see the evidence register)* *"4.4 Terms of employment, conduct and termination 4.4.1 Employment contracts and contractor agreements shall include confidentiality, acceptable-use and security responsibilities that survive termination of employment."* 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.
A.6.6	Confidentiality or non-disclosure agreements	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
A.6.7	Remote working	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	046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 032_operational_resilience_policy_cps_230.pdf · `4027f4cd46d7…` 043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` *+ 1 more cited (see the evidence register)* *"Purpose and control objectives This procedure establishes the requirements, accountabilities and control objectives for personnel security screening, onboarding & offboarding procedure across Southern Mutual Bank ("the Bank")."* 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.
A.6.8	Information security event reporting	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	008_logging_monitoring_policy.pdf · `808a97e670d8…` *"4.8 Monitoring, measurement and reporting 4.8.1 Control performance shall be monitored continuously through automated telemetry into the central assurance platform."* 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.

*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.*

Physical (14)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
A.7.1	Physical security perimeters	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	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 041_physical_environmental_security_policy.pdf · `d0fa967acaaf…` *"Control objectives: • Prevent unauthorised physical access to facilities, secure areas, equipment and media through layered physical security and physical protection controls."* 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
A.7.2	Physical entry	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	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183`… 041_physical_environmental_security_policy.pdf · `d0fa967acaaf`… 1229_privileged_access_configuration_export_pam_platform.pdf · `31e96f8caef6`… *+ 1 more cited (see the evidence register)* *"Requirements 4.1 Physical access control and secure areas 4.1.1 Physical access to data centres, communications rooms and other secure areas shall be restricted to authorised personnel using access cards, PIN and, for the highest-security rooms, biometric physical access control."* 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.
A.7.3	Securing offices, rooms and facilities	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`… *"Control objectives: • Maintain an accurate, owned and classified inventory of information assets."* 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.
A.7.4	Physical security monitoring	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	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183`… 041_physical_environmental_security_policy.pdf · `d0fa967acaaf`… 1229_privileged_access_configuration_export_pam_platform.pdf · `31e96f8caef6`… *+ 2 more cited (see the evidence register)* *"Control objectives: • Prevent unauthorised physical access to facilities, secure areas, equipment and media through layered physical security and physical protection controls."* 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
A.7.5	Protecting against physical and environmental threats	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	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 041_physical_environmental_security_policy.pdf · `d0fa967acaaf…` *"4.2 Physical and environmental protection of equipment 4.2.1 Physical and environmental controls shall protect equipment against fire, flood, power failure and temperature or humidity excursions: fire detection and suppression, dual power feeds with UPS and generator, and environmental monitoring with alerting."* 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.
A.7.6	Working in secure areas	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	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 041_physical_environmental_security_policy.pdf · `d0fa967acaaf…` *"Control objectives: • Prevent unauthorised physical access to facilities, secure areas, equipment and media through layered physical security and physical protection controls."* 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.
A.7.7	Clear desk and clear screen	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	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 041_physical_environmental_security_policy.pdf · `d0fa967acaaf…` *"4.2.3 Equipment, media and paper records shall be protected against theft and unauthorised viewing through a clear-desk and clear-screen rule, locked storage for classified material and secure cabling routes."* 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
A.7.8	Equipment siting and protection	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`… *"4.1.3 Unauthorised, unmanaged and end-of-life assets shall be identified and remediated."* 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.
A.7.9	Security of assets off-premises	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`… *"Control objectives: • Maintain an accurate, owned and classified inventory of information assets."* 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.
A.7.10	Storage media	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`… *"4.2.2 Handling, storage, transmission and sharing controls shall be applied per classification."* 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.
A.7.11	Supporting utilities	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	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183`… 041_physical_environmental_security_policy.pdf · `d0fa967acaaf`… 1228_multi_factor_authentication_configuration_export_entra_id_tenant.pdf · `dd3b9d2f6e6a`… *+ 1 more cited (see the evidence register)* *"4.7.2 Supporting utilities (power, cooling, water, telecommunications) shall have redundancy proportionate to the criticality of the equipment they serve and shall be tested on a defined schedule."* 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
A.7.12	Cabling security	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	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183`… 041_physical_environmental_security_policy.pdf · `d0fa967acaaf`… *"4.7.2 Supporting utilities (power, cooling, water, telecommunications) shall have redundancy proportionate to the criticality of the equipment they serve and shall be tested on a defined schedule."* 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.
A.7.13	Equipment maintenance	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	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183`… 041_physical_environmental_security_policy.pdf · `d0fa967acaaf`… *"4.2.4 Equipment taken off-site shall be authorised, recorded and protected in transit; equipment and media shall be sanitised before reuse or disposal."* 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.
A.7.14	Secure disposal or re-use of equipment	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`… *"4.3 Disposal and media 4.3.1 Media shall be sanitised or destroyed to an approved standard before disposal or reuse."* 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.*

Technological (34)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
A.8.1	User endpoint devices	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** confirmed	050_secure_system_build_hardening_procedure.pdf · `cf44bbd2d2df…` 035_endpoint_protection_standard.pdf · `d0f5b621bd23…` 017_secure_configuration_baseline_standard.pdf · `5fcfa2208092…` *+ 2 more cited (see the evidence register)* *"firewall and endpoint protection enforced when connected to untrusted networks Compliant Device encryption Full-disk encryption on; recovery keys escrowed Compliant Hardening baseline compliance 1203 of 1244 devices compliant with the endpoint hardening baseline Partially compliant — 52 drifted, remediation ticketed"* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Partially implemented (exception)	User endpoint devices — touched by the evidence assessed against it (5 cited documents) but not established by it. (evidence route: uploaded evidence) — Remediate and provide evidence for re-validation.
A.8.2	Privileged access rights	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** confirmed	1229_privileged_access_configuration_export_pam_platform.pdf · `31e96f8caef6…` 1228_multi_factor_authentication_configuration_export_entra_id_tenant.pdf · `dd3b9d2f6e6a…` 221_endpoint_protection_console_export_payments_switch.pdf · `b7d7ab942d91…` *+ 2 more cited (see the evidence register)* *"any use Compliant Least privilege — role definitions 42 privileged roles defined; access control rights reviewed quarterly Compliant"* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Partially implemented (exception)	Privileged access rights — touched by the evidence assessed against it (5 cited documents) but not established by it. (evidence route: uploaded evidence) — Remediate and provide evidence for re-validation.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
A.8.3	Information access restriction	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)	221_endpoint_protection_console_export_payments_switch.pdf · `b7d7ab942d91`… 131_endpoint_protection_console_export_internet_banking.pdf · `e850c4525d85`… 1229_privileged_access_configuration_export_pam_platform.pdf · `31e96f8caef6`… *+ 2 more cited (see the evidence register)* *"any use Compliant Least privilege — role definitions 42 privileged roles defined; access control rights reviewed quarterly Compliant"* 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.
A.8.4	Access to source code	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	053_security_testing_assurance_procedure.pdf · `62b4dd18699d`… 050_secure_system_build_hardening_procedure.pdf · `cf44bbd2d2df`… 001_information_security_policy.pdf · `19b799381535`… *+ 1 more cited (see the evidence register)* *"Control objectives: • Build security into the software development lifecycle (SDLC) so applications are secure by design and secure coding is verified before release."* 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.
A.8.5	Secure authentication	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	053_security_testing_assurance_procedure.pdf · `62b4dd18699d`… 002_access_control_policy.pdf · `b0d755704774`… 001_information_security_policy.pdf · `19b799381535`… *+ 1 more cited (see the evidence register)* *"4.2 Authentication and credentials 4.2.1 Multi-factor authentication (MFA) shall be enforced for all remote, administrative, internet-facing and customer access, using phishing-resistant factors where supported."* 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
A.8.6	Capacity 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	008_logging_monitoring_policy.pdf · `808a97e670d8…` 1224_application_control_event_log_extract_workstations_q2_2026.pdf · `d8c9185aed67…` 117_soc_monitoring_report_q2_2026.pdf · `06ca0cc7ca28…` *+ 1 more cited (see the evidence register)* *"Summary of results Security events ingested into the SIEM 1.2 billion — event logs, audit logs, network and identity sources; log retention 12 months Alerts triaged (security monitoring, intrusion detection, anomaly detection) 3,418 Alerts triaged within SLA 97.8% — alerting reviewed by the 24x7 security operations centre Escalated to security incident 6 — continuous monitoring use cases reviewed"* 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.
A.8.7	Protection against malware	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)	1240_powershell_and_process_creation_auditing_configuration_export_windows_fleet.pdf · `9e603bbcafff…` 1226_browser_and_pdf_reader_hardening_configuration_export_workstations.pdf · `59c5e77d31b9…` 1235_wdac_application_control_policy_configuration_export_workstations_and_servers.pdf · `c128df5d52ea…` *+ 2 more cited (see the evidence register)* *"software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets Compliant Rule types Publisher certificate rules and file hash rules; path rules only for admin-writable locations; user profile, temporary and download folders blocked Compliant Microsoft recommended block rules Merged into the policy — current list applied 30 Sep 2026 Compliant Driver control —"* 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
A.8.8	Management of technical vulnerabilities	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…` 202_patch_compliance_report_core_banking_temenos_t24_q3_2025.pdf · `54433d09b730…` *+ 2 more cited (see the evidence register)* *"Results Host CVE CVSS / severity Vulnerability Remediation status Evidence db-host-01 CVE-2026-3513 Critical 9.8 Missing security patch — vendor advisory OPEN — beyond SLA Patch record CHG-208300 web-host-02 CVE-2026-5905 High 7.5 Unsupported software version Remediated 18 Oct 2026 Patch record CHG-208301 web-host-03 CVE-2026-9021 Critical 9.8 Default credentials Remediated 17 Oct 2026 Patch"* 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.
A.8.9	Configuration management	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** confirmed	221_endpoint_protection_console_export_payments_switch.pdf · `b7d7ab942d91…` 131_endpoint_protection_console_export_internet_banking.pdf · `e850c4525d85…` 1240_powershell_and_process_creation_auditing_configuration_export_windows_fleet.pdf · `9e603bbcafff…` *+ 2 more cited (see the evidence register)* *"What this export is A configuration export for Workstations and Servers: the current settings as held by the system, section by section, with the compliance status against the applicable baseline."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Partially implemented (exception)	Configuration management — touched by the evidence assessed against it (5 cited documents) but not established by it. (evidence route: uploaded evidence) — Remediate and provide evidence for re-validation.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
A.8.10	Information deletion	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	046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 047_personal_information_handling_procedure.pdf · `dc109a6f6de6…` 011_data_breach_response_procedure.pdf · `4bc5e0e094ad…` *+ 2 more cited (see the evidence register)* *"■ Meet obligations under the Privacy Act and the Notifiable Data Breaches scheme."* 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.
A.8.11	Data masking	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	022_privacy_policy.pdf · `e9579dc88cc5…` 038_data_retention_disposal_standard.pdf · `7763782c1a38…` 100_privacy_data_protection_configuration_export_core_banking_temenos_t24.pdf · `be04d860281c…` *+ 2 more cited (see the evidence register)* *"Data leakage prevention (DLP) Setting Value Status DLP on endpoints Endpoint DLP agent on all managed devices: sensitive-data patterns (personal information, cardholder data) blocked from removable media and unapproved cloud storage Compliant DLP on email and web Email DLP rules quarantine outbound messages carrying unapproved sensitive data; web gateway DLP inspects uploads Compliant DLP on"* 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
A.8.12	Data leakage prevention	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** confirmed	100_privacy_data_protection_configuration_export_core_banking_temenos_t24.pdf · `be04d860281c…` *"Data leakage prevention (DLP) Setting Value Status DLP on endpoints Endpoint DLP agent on all managed devices: sensitive-data patterns (personal information, cardholder data) blocked from removable media and unapproved cloud storage Compliant DLP on email and web Email DLP rules quarantine outbound messages carrying unapproved sensitive data; web gateway DLP inspects uploads Compliant DLP on"* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Partially implemented (exception)	Data leakage prevention — touched by the evidence assessed against it (1 cited document) but not established by it. (evidence route: uploaded evidence) — Remediate and provide evidence for re-validation.
A.8.13	Information backup	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** confirmed	133_backup_jobs_report_core_banking_temenos_t24_q2_2026.pdf · `07156e0422ea…` *"Protection of backups Setting Value Status Modification and deletion Backups protected so only backup administrators can modify or delete them Compliant Immutable and offline copies Immutable object-lock copies (30 days) and offline copies against ransomware Compliant Alternate storage site Backups replicated to an alternate storage site in a separate region; agreements in place for storage and"* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Partially implemented (exception)	Information backup — touched by the evidence assessed against it (1 cited document) but not established by it. (evidence route: uploaded evidence) — Remediate and provide evidence for re-validation.
A.8.14	Redundancy of information processing facilities	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…` 014_backup_restoration_standard.pdf · `9342ac709c37…` 100_privacy_data_protection_configuration_export_core_banking_temenos_t24.pdf · `be04d860281c…` *"This reduces the likelihood and impact of unauthorised access or control failure."* 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
A.8.15	Logging	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)	008_logging_monitoring_policy.pdf · `808a97e670d8…` 1224_application_control_event_log_extract_workstations_q2_2026.pdf · `d8c9185aed67…` 117_soc_monitoring_report_q2_2026.pdf · `06ca0cc7ca28…` *+ 1 more cited (see the evidence register)* *"Summary of results Security events ingested into the SIEM 1.2 billion — event logs, audit logs, network and identity sources; log retention 12 months Alerts triaged (security monitoring, intrusion detection, anomaly detection) 3,418 Alerts triaged within SLA 97.8% — alerting reviewed by the 24x7 security operations centre Escalated to security incident 6 — continuous monitoring use cases reviewed"* 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.
A.8.16	Monitoring activities	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** confirmed	008_logging_monitoring_policy.pdf · `808a97e670d8…` 117_soc_monitoring_report_q2_2026.pdf · `06ca0cc7ca28…` 207_soc_monitoring_report_q3_2025.pdf · `bace47f7be25…` *"Summary of results Security events ingested into the SIEM 1.2 billion — event logs, audit logs, network and identity sources; log retention 12 months Alerts triaged (security monitoring, intrusion detection, anomaly detection) 3,418 Alerts triaged within SLA 97.8% — alerting reviewed by the 24x7 security operations centre Escalated to security incident 6 — continuous monitoring use cases reviewed"* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Partially implemented (exception)	Monitoring activities — touched by the evidence assessed against it (3 cited documents) but not established by it. (evidence route: uploaded evidence) — Remediate and provide evidence for re-validation.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
A.8.17	Clock synchronisation	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	008_logging_monitoring_policy.pdf · `808a97e670d8…` 1235_wdac_application_control_policy_configuration_export_workstations_and_servers.pdf · `c128df5d52ea…` 1224_application_control_event_log_extract_workstations_q2_2026.pdf · `d8c9185aed67…` *+ 2 more cited (see the evidence register)* *"Southern Mutual Bank — Internal Use Only · UNCONTROLLED WHEN PRINTED · SYNTHETIC TEST DOCUMENT Page 2 4.1.1 Security-relevant events shall be centrally collected, time-synchronised (NTP) and retained for at least 12 months (and longer where regulation requires)."* 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.
A.8.18	Use of privileged utility programs	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)	1240_powershell_and_process_creation_auditing_configuration_export_windows_fleet.pdf · `9e603bbcafff…` 221_endpoint_protection_console_export_payments_switch.pdf · `b7d7ab942d91…` 131_endpoint_protection_console_export_internet_banking.pdf · `e850c4525d85…` *+ 2 more cited (see the evidence register)* *"PowerShell Setting Value Status PowerShell script block logging On — all hosts; events forwarded to the SIEM Compliant PowerShell module logging and transcription On — transcripts written to a protected share Compliant PowerShell 2.0 Removed from all workstations and servers Compliant PowerShell language mode Constrained language mode for non-administrators, enforced by application control"* 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
A.8.19	Installation of software on operational systems	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** confirmed	050_secure_system_build_hardening_procedure.pdf · `cf44bbd2d2df…` 017_secure_configuration_baseline_standard.pdf · `5fcfa2208092…` 016_patch_management_standard.pdf · `7d5c195985fd…` *+ 2 more cited (see the evidence register)* *"Device hardening Setting Value Status Application control / allowlisting Enforced — only authorised software runs; unauthorised software removed Compliant Collaborative computing devices (camera, microphone) Remote activation prohibited; explicit indication of use (indicator light) to users present Compliant Dual-connected devices (untrusted network and CDE) Split tunnelling prohibited; host"* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Partially implemented (exception)	Installation of software on operational systems — touched by the evidence assessed against it (5 cited documents) but not established by it. (evidence route: uploaded evidence) — Remediate and provide evidence for re-validation.
A.8.20	Networks security	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)	221_endpoint_protection_console_export_payments_switch.pdf · `b7d7ab942d91…` 131_endpoint_protection_console_export_internet_banking.pdf · `e850c4525d85…` 222_secure_configuration_export_payments_switch.pdf · `6f971a57866a…` *"System security parameters Setting Value Status Secure configuration baseline applied CIS Level 1 baseline for Payments Switch; system security parameters configured to prevent misuse Compliant Insecure services and protocols Present: legacy FTP on host b-07 — business justification documented, additional safeguards (network isolation, monitoring) applied; retirement scheduled Justified 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.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
A.8.21	Security of network services	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	008_logging_monitoring_policy.pdf · `808a97e670d8…` 1224_application_control_event_log_extract_workstations_q2_2026.pdf · `d8c9185aed67…` 117_soc_monitoring_report_q2_2026.pdf · `06ca0cc7ca28…` *"Summary of results Security events ingested into the SIEM 1.2 billion — event logs, audit logs, network and identity sources; log retention 12 months Alerts triaged (security monitoring, intrusion detection, anomaly detection) 3,418 Alerts triaged within SLA 97.8% — alerting reviewed by the 24x7 security operations centre Escalated to security incident 6 — continuous monitoring use cases reviewed"* 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.
A.8.22	Segregation of networks	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
A.8.23	Web filtering	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** confirmed	221_endpoint_protection_console_export_payments_switch.pdf · `b7d7ab942d91`… 131_endpoint_protection_console_export_internet_banking.pdf · `e850c4525d85`… 1229_privileged_access_configuration_export_pam_platform.pdf · `31e96f8caef6`… *+ 2 more cited (see the evidence register)* *"Southern Mutual Bank — Internal Use Only · UNCONTROLLED WHEN PRINTED · SYNTHETIC TEST DOCUMENT Page 2 Setting Value Status DNS and web filtering DNS filtering and web gateway category blocking; network traffic to malicious domains blocked Compliant 4."* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Partially implemented (exception)	Web filtering — touched by the evidence assessed against it (5 cited documents) but not established by it. (evidence route: uploaded evidence) — Remediate and provide evidence for re-validation.
A.8.24	Use of cryptography	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.
A.8.25	Secure development life cycle	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	053_security_testing_assurance_procedure.pdf · `62b4dd18699d`… 050_secure_system_build_hardening_procedure.pdf · `cf44bbd2d2df`… 017_secure_configuration_baseline_standard.pdf · `5fcfa2208092`… *+ 1 more cited (see the evidence register)* *"Control objectives: • Build security into the software development lifecycle (SDLC) so applications are secure by design and secure coding is verified before release."* 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
A.8.26	Application security requirements	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	053_security_testing_assurance_procedure.pdf · `62b4dd18699d`… 002_access_control_policy.pdf · `b0d755704774`… 025_network_security_policy.pdf · `99f3533716db`… *+ 1 more cited (see the evidence register)* *"4.1.3 Security testing shall be performed before release: static application security testing (SAST) on every build, software composition analysis for dependencies, dynamic testing (DAST) on staging and penetration testing for internet-facing or high-risk applications."* 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.
A.8.27	Secure system architecture and engineering principles	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	053_security_testing_assurance_procedure.pdf · `62b4dd18699d`… 050_secure_system_build_hardening_procedure.pdf · `cf44bbd2d2df`… 017_secure_configuration_baseline_standard.pdf · `5fcfa2208092`… *+ 1 more cited (see the evidence register)* *"Requirements 4.1 Secure development lifecycle 4.1.1 A secure development lifecycle shall be defined for all in-house and outsourced software development, with security requirements, threat modelling and security by design activities at each phase."* 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
A.8.28	Secure coding	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	053_security_testing_assurance_procedure.pdf · `62b4dd18699d…` 008_logging_monitoring_policy.pdf · `808a97e670d8…` 1222_application_control_allowlist_review_approval_and_sign_off_record_q2_2026.pdf · `c1a53b33df4a…` *"Control objectives: • Build security into the software development lifecycle (SDLC) so applications are secure by design and secure coding is verified before release."* 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.
A.8.29	Security testing in development and acceptance	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	053_security_testing_assurance_procedure.pdf · `62b4dd18699d…` 050_secure_system_build_hardening_procedure.pdf · `cf44bbd2d2df…` 017_secure_configuration_baseline_standard.pdf · `5fcfa2208092…` *+ 1 more cited (see the evidence register)* *"Southern Mutual Bank — Internal Use Only · UNCONTROLLED WHEN PRINTED · SYNTHETIC TEST DOCUMENT Page 2 4.1 Vulnerability identification 4.1.1 Authenticated vulnerability scanning shall be performed at least monthly across the estate; internet-facing assets weekly."* 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.
A.8.30	Outsourced development	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	019_third_party_risk_management_policy.pdf · `dc41ed8ba096…` 008_logging_monitoring_policy.pdf · `808a97e670d8…` 002_access_control_policy.pdf · `b0d755704774…` *+ 1 more cited (see the evidence register)* *"Control objectives: • Ensure third parties and material service providers meet the organisation's security and resilience obligations."* 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
A.8.31	Separation of development, test and production environments	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	053_security_testing_assurance_procedure.pdf · `62b4dd18699d…` 050_secure_system_build_hardening_procedure.pdf · `cf44bbd2d2df…` 017_secure_configuration_baseline_standard.pdf · `5fcfa2208092…` *+ 1 more cited (see the evidence register)* *"4.1.4 Development, test and production environments shall be segregated; production data shall not be used in development or test without masking and approval."* 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.
A.8.32	Change 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	053_security_testing_assurance_procedure.pdf · `62b4dd18699d…` 008_logging_monitoring_policy.pdf · `808a97e670d8…` 1222_application_control_allowlist_review_approval_and_sign_off_record_q2_2026.pdf · `c1a53b33df4a…` *+ 2 more cited (see the evidence register)* *"4.3.3 Release to production shall require evidence of passed security testing, completed code review and an approved change record; releases shall be deployable by pipeline only, never by hand."* 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
A.8.33	Test information	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	053_security_testing_assurance_procedure.pdf · `62b4dd18699d…` 1240_powershell_and_process_creation_auditing_configuration_export_windows_fleet.pdf · `9e603bbcafff…` 1235_wdac_application_control_policy_configuration_export_workstations_and_servers.pdf · `c128df5d52ea…` *+ 1 more cited (see the evidence register)* *"4.1.4 Development, test and production environments shall be segregated; production data shall not be used in development or test without masking and approval."* 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.
A.8.34	Protection of information systems during audit testing	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	008_logging_monitoring_policy.pdf · `808a97e670d8…` 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.

*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.*

3a. 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.

Access Control	0 of 9 Implemented / operating effectively (0%) — 1 Partially implemented (exception), 8 Candidate evidence — assessor review
Data Protection	0 of 16 Implemented / operating effectively (0%) — 3 Partially implemented (exception), 2 Insufficient evidence, 2 Manual assessment required, 9 Candidate evidence — assessor review
Network Security	0 of 4 Implemented / operating effectively (0%) — 1 Partially implemented (exception), 1 Manual assessment required, 2 Candidate evidence — assessor review
Threat Detection	0 of 10 Implemented / operating effectively (0%) — 1 Partially implemented (exception), 3 Insufficient evidence, 6 Candidate evidence — assessor review
Incident Response	0 of 9 Implemented / operating effectively (0%) — 2 Insufficient evidence, 7 Candidate evidence — assessor review
Governance & Risk	0 of 20 Implemented / operating effectively (0%) — 5 Insufficient evidence, 1 Manual assessment required, 14 Candidate evidence — assessor review
Physical & Environmental	0 of 13 Implemented / operating effectively (0%) — 2 Insufficient evidence, 11 Candidate evidence — assessor review
Personnel Security	0 of 7 Implemented / operating effectively (0%) — 7 Candidate evidence — assessor review
Asset & Configuration	0 of 7 Implemented / operating effectively (0%) — 2 Partially implemented (exception), 2 Insufficient evidence, 1 Manual assessment required, 2 Candidate evidence — assessor review
Application Security	0 of 8 Implemented / operating effectively (0%) — 8 Candidate evidence — assessor review
Supply Chain / Third-Party	0 of 5 Implemented / operating effectively (0%) — 2 Insufficient evidence, 3 Candidate evidence — assessor review
Other	0 of 8 Implemented / operating effectively (0%) — 4 Manual assessment required, 4 Candidate evidence — assessor review

3b. 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.

3c. 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
Organizational	Evidence on file — % of catalogue	97% of catalogue have evidence on file · 0 verified	0/37	36	0	12	1
People	Verified — % of catalogue	0% of catalogue verified	0/8	7	0	1	1
Physical	Evidence on file — % of catalogue	100% of catalogue have evidence on file · 0 verified	0/14	14	0	3	0

Pillar	Lead KPI	Value	Verified	Evidence on file	At risk	Evidence gap / no visibility	Unassessed
Technological	Evidence on file — % of catalogue	94% of catalogue have evidence on file · 0 verified	0/34	32	0	2	2
Management system (clauses 4–10)	Verified — % of catalogue	0% of catalogue verified	0/23	18	0	0	5

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: 18 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.

4. Statement of Applicability

This section is the control-by-control basis for the Statement of Applicability: every Annex A control with its resolved requirement text and its assessed status. A complete SoA additionally records, per control, the applicability DECISION and its justification (including exclusions) — an assessor judgement this engine does not make. CyberSentien issues the SoA itself as the companion artefact named on the report-format page.

The assessed controls with their requirement text, for the 93 controls not reported under a theme section above. Organisation-defined parameters are resolved to the baseline value where set, or shown as the precise descriptor (e.g. [organization-defined frequency]) where the baseline leaves them to the organisation. The result assessed for each is shown beside it.

Organizational

A.5.1 — Policies for information security — Candidate evidence — assessor review

Define, approve at management level, publish and communicate an information security policy set aligned to business objectives, and review it at planned intervals and on significant change; policy framework, governance.

A.5.2 — Information security roles and responsibilities — Candidate evidence — assessor review

Define and allocate specific information security responsibilities to individuals so accountability is clear and there are no ownership gaps; RACI, role assignment, governance structure.

A.5.3 — Segregation of duties — Candidate evidence — assessor review

Separate conflicting duties and areas of responsibility so no single person can misuse a critical process; segregation of duties, dual control, fraud prevention.

A.5.4 — Management responsibilities — Candidate evidence — assessor review

Require management to actively support and enforce information security, allocating resources and ensuring all personnel apply the policies, procedures and standards.

A.5.5 — Contact with authorities — Insufficient evidence

Establish and maintain contact with relevant authorities such as regulators, law enforcement and CERTs to enable rapid, lawful response to incidents and obligations.

A.5.6 — Contact with special interest groups — Candidate evidence — assessor review

Maintain contact with security forums, special interest groups and professional associations to stay current on threats and good practice.

A.5.7 — Threat intelligence — Insufficient evidence

Collect and analyse information about security threats, including feeds and indicators of compromise, to inform risk decisions and adjust defences proactively; tactical, operational and strategic intelligence.

A.5.8 — Information security in project management — Insufficient evidence

Integrate information security into project management for all projects, defining security requirements and assessing risk early so deliverables are secure by design.

A.5.9 — Inventory of information and other associated assets — Insufficient evidence

Identify and maintain an inventory of information and associated assets with owners; asset register, CMDB, data inventory, basis for risk assessment.

A.5.10 — Acceptable use of information and other associated assets — Candidate evidence — assessor review

Define and enforce rules for the acceptable use and handling of information and assets to prevent misuse, damage or unauthorised access; acceptable use policy.

A.5.11 — Return of assets — Manual assessment required

Ensure personnel and contractors return all organisational assets on termination or change of employment to prevent data leakage; asset return checklist.

A.5.12 — Classification of information — Insufficient evidence

Classify information by confidentiality, integrity, availability, value and legal requirements so appropriate protection is applied; data classification scheme.

A.5.13 — Labelling of information — Candidate evidence — assessor review

Label information in line with the classification scheme so people and systems can identify sensitivity and handle it correctly; sensitivity labels, markings.

A.5.14 — Information transfer — Candidate evidence — assessor review

Establish rules, procedures and agreements to protect information transferred within and outside the organisation; secure transfer, encryption, transfer agreements, secure email.

A.5.15 — Access control — Candidate evidence — assessor review

Establish and implement rules to control physical and logical access to information based on business and security requirements; access control policy, least privilege, need to know.

A.5.16 — Identity management — Candidate evidence — assessor review

Manage the full lifecycle of identities including registration, provisioning, changes and de-provisioning so every action is accountable; identity governance, unique IDs, joiner/mover/leaver.

A.5.17 — Authentication information — Candidate evidence — assessor review

Control the allocation and management of authentication information such as passwords, secrets and MFA factors; credential management, password policy, secret rotation.

A.5.18 — Access rights — Candidate evidence — assessor review

Provision, review, modify and revoke access rights per policy so access matches current roles; periodic access review, recertification, revocation on leaving, prevention of permission creep.

A.5.19 — Information security in supplier relationships — Insufficient evidence

Define and apply processes to manage the information security risks arising from supplier products and services; third-party and vendor risk management.

A.5.20 — Addressing information security within supplier agreements — Candidate evidence — assessor review

Establish and agree relevant information security requirements with each supplier and embed them in contracts; security clauses, incident reporting obligations.

A.5.21 — Managing information security in the ICT supply chain — Insufficient evidence

Manage security risks across the ICT products and services supply chain, requiring assurance over the integrity of hardware and software components.

A.5.22 — Monitoring, review and change management of supplier services — Candidate evidence — assessor review

Regularly monitor, review and audit supplier service delivery against agreements and manage changes to their services securely; SLA and assurance reviews.

A.5.23 — Information security for use of cloud services — Candidate evidence — assessor review

Establish processes for acquisition, use, management and exit of cloud services under the shared-responsibility model; cloud security, CSP responsibilities, exit strategy.

A.5.24 — Information security incident management planning and preparation — Candidate evidence — assessor review

Plan and prepare incident management by defining process, roles and responsibilities so incidents are detected, reported, assessed and responded to effectively; incident response plan.

A.5.25 — Assessment and decision on information security events — Candidate evidence — assessor review

Assess security events and decide whether to classify them as incidents so the right response is triggered; triage, categorisation.

A.5.26 — Response to information security incidents — Candidate evidence — assessor review

Respond to confirmed incidents per documented procedures including containment, eradication and recovery, and keep records; incident handling.

A.5.27 — Learning from information security incidents — Insufficient evidence

Use knowledge gained from incidents to strengthen controls and reduce recurrence; post-incident review, root-cause analysis, lessons learned.

A.5.28 — Collection of evidence — Candidate evidence — assessor review

Define procedures to identify, collect, acquire and preserve evidence with integrity and chain of custody for disciplinary or legal action; forensic readiness.

A.5.29 — Information security during disruption — Candidate evidence — assessor review

Maintain information security at an appropriate level during disruption, or replace controls with equivalent measures during emergency operation; resilience of controls.

A.5.30 — ICT readiness for business continuity — Candidate evidence — assessor review

Plan, implement, maintain and test ICT continuity so systems meet business continuity objectives; disaster recovery, RTO/RPO, redundancy, DR testing.

A.5.31 — Legal, statutory, regulatory and contractual requirements — Insufficient evidence

Identify, document and keep current all legal, statutory, regulatory and contractual requirements and the approach to meet them; compliance obligations register.

A.5.32 — Intellectual property rights — Insufficient evidence

Implement procedures to protect intellectual property rights and ensure compliance with licensing and IP law; software licence compliance.

A.5.33 — Protection of records — Candidate evidence — assessor review

Protect records from loss, destruction, falsification, unauthorised access and unauthorised release in line with legal, regulatory and business needs; retention, records management.

A.5.34 — Privacy and protection of PII — Candidate evidence — assessor review

Identify and meet requirements for the privacy and protection of personally identifiable information through technical and organisational measures; privacy controls, GDPR and privacy law.

A.5.35 — Independent review of information security — Insufficient evidence

Have the information security approach and its implementation reviewed independently at planned intervals and on significant change; internal and external audit.

A.5.36 — Compliance with policies, rules and standards for information security — Insufficient evidence

Regularly review compliance with the organisation's information security policies, rules and standards; control testing, compliance checking.

A.5.37 — Documented operating procedures — Candidate evidence — assessor review

Document operating procedures for information processing facilities and make them available to those who need them; runbooks, SOPs, consistency, reduced human error.

People

A.6.1 — Screening — Candidate evidence — assessor review

Carry out background verification checks on candidates proportionate to information classification, before and during employment; vetting, screening, insider-threat mitigation.

A.6.2 — Terms and conditions of employment — Candidate evidence — assessor review

State personnel and organisational information security responsibilities in employment agreements; confidentiality and data-protection obligations.

A.6.3 — Information security awareness, education and training — Candidate evidence — assessor review

Provide personnel with security awareness, education and training relevant to their role and updated regularly; awareness programme, phishing training.

A.6.4 — Disciplinary process — Candidate evidence — assessor review

Operate a formal, communicated disciplinary process to take action against personnel who commit a security policy violation; deterrence.

A.6.5 — Responsibilities after termination or change of employment — Candidate evidence — assessor review

Define, communicate and enforce security responsibilities that remain valid after termination or change of employment; access revocation, continuing confidentiality.

A.6.6 — Confidentiality or non-disclosure agreements — Manual assessment required

Identify, document, review and have signed confidentiality or non-disclosure agreements reflecting the organisation's needs; NDAs for staff and third parties.

A.6.7 — Remote working — Candidate evidence — assessor review

Implement security measures for personnel working remotely to protect information accessed, processed or stored off-site; teleworking policy, VPN, device encryption.

A.6.8 — Information security event reporting — Insufficient evidence

Provide a mechanism for personnel to report observed or suspected information security events promptly through appropriate channels; event reporting.

Physical

A.7.1 — Physical security perimeters — Candidate evidence — assessor review

Define and use security perimeters to protect areas that contain information and associated assets; walls, barriers, controlled entry points.

A.7.2 — Physical entry — Candidate evidence — assessor review

Protect secure areas with appropriate entry controls and access points; badge or biometric access, visitor management, entry logs.

A.7.3 — Securing offices, rooms and facilities — Insufficient evidence

Design and apply physical security for offices, rooms and facilities that hold information and assets; locks, layout, protection from theft and eavesdropping.

A.7.4 — Physical security monitoring — Candidate evidence — assessor review

Continuously monitor premises for unauthorised physical access; CCTV, intrusion alarms, motion sensors, guards, recorded audit trail.

A.7.5 — Protecting against physical and environmental threats — Candidate evidence — assessor review

Design and implement protection against physical and environmental threats such as fire, flood, earthquake and civil unrest; environmental controls.

A.7.6 — Working in secure areas — Candidate evidence — assessor review

Design and apply security measures for working in secure areas; supervision, restrictions on recording, controlled activity.

A.7.7 — Clear desk and clear screen — Candidate evidence — assessor review

Enforce clear-desk rules for papers and removable media and clear-screen rules for information processing facilities; lock-away, screen lock.

A.7.8 — Equipment siting and protection — Insufficient evidence

Site and protect equipment to reduce risks from physical and environmental threats and unauthorised viewing; positioning, screen privacy.

A.7.9 — Security of assets off-premises — Candidate evidence — assessor review

Protect assets used or stored off-site through physical protection, encryption and usage rules; mobile devices, off-premises equipment.

A.7.10 — Storage media — Insufficient evidence

Manage removable and other storage media through classification, handling, transport and secure disposal; media handling procedures, sanitisation.

A.7.11 — Supporting utilities — Candidate evidence — assessor review

Protect facilities from disruption caused by failures of supporting utilities such as power and telecommunications; UPS, backup generators, redundancy.

A.7.12 — Cabling security — Candidate evidence — assessor review

Protect power and telecommunications cabling carrying data or supporting services from interception, interference and damage; secure routing, shielding.

A.7.13 — Equipment maintenance — Candidate evidence — assessor review

Maintain equipment correctly and under control to ensure continued availability, integrity and confidentiality; supervised maintenance, authorised repairs.

A.7.14 — Secure disposal or re-use of equipment — Candidate evidence — assessor review

Verify that equipment containing storage media has sensitive data and licensed software securely removed or overwritten before disposal or re-use; media sanitisation, secure wipe.

Technological

A.8.1 — User endpoint devices — Partially implemented (exception)

Protect information stored on, processed by or accessible via user endpoint devices; endpoint security, encryption, device management, MDM, hardening.

A.8.2 — Privileged access rights — Partially implemented (exception)

Restrict and manage the allocation and use of privileged access rights; admin accounts, PAM, least privilege, privileged access review.

A.8.3 — Information access restriction — Candidate evidence — assessor review

Restrict access to information and application functions per the access control policy; need to know, least privilege, function-level restriction.

A.8.4 — Access to source code — Candidate evidence — assessor review

Appropriately manage read and write access to source code, development tools and software libraries; source-code repository access control.

A.8.5 — Secure authentication — Candidate evidence — assessor review

Implement secure authentication technologies and procedures based on access restrictions; multi-factor authentication, MFA, conditional access, strong authentication.

A.8.6 — Capacity management — Candidate evidence — assessor review

Monitor and tune the use of resources against current and projected capacity requirements to maintain performance and availability; capacity planning.

A.8.7 — Protection against malware — Candidate evidence — assessor review

Implement protection against malware supported by user awareness; anti-malware, endpoint protection, EDR, file scanning, detection and recovery.

A.8.8 — Management of technical vulnerabilities — Insufficient evidence

Obtain information about technical vulnerabilities, evaluate exposure and take timely action; vulnerability scanning, patch management, CVE/CVSS, remediation SLAs.

A.8.9 — Configuration management — Partially implemented (exception)

Establish, document, implement, monitor and review secure configurations of hardware, software, services and networks; secure baselines, hardening, configuration and change control.

A.8.10 — Information deletion — Candidate evidence — assessor review

Delete information held in systems, devices and media when no longer required to reduce exposure and meet legal obligations; secure deletion, data disposal.

A.8.11 — Data masking — Candidate evidence — assessor review

Use data masking in line with access control policy to limit exposure of sensitive data including PII; anonymisation, pseudonymisation, tokenisation, test-data masking.

A.8.12 — Data leakage prevention — Partially implemented (exception)

Apply data leakage prevention measures across systems, networks, endpoints and email to detect and prevent unauthorised disclosure of sensitive information; DLP.

A.8.13 — Information backup — Partially implemented (exception)

Maintain and regularly test backups of information, software and systems per an agreed backup policy; backup and restore testing, recovery from ransomware or failure, offline copies.

A.8.14 — Redundancy of information processing facilities — Candidate evidence — assessor review

Implement information processing facilities with redundancy to meet availability requirements; failover, high availability, elimination of single points of failure.

A.8.15 — Logging — Candidate evidence — assessor review

Produce, store, protect and analyse logs of activities, exceptions, faults and security events; audit logging, log retention, tamper protection.

A.8.16 — Monitoring activities — Partially implemented (exception)

Monitor networks, systems and applications for anomalous behaviour and act to evaluate potential incidents; security monitoring, SIEM, detection, alerting.

A.8.17 — Clock synchronisation — Candidate evidence — assessor review

Synchronise the clocks of information processing systems to approved time sources so logs and events correlate accurately; NTP.

A.8.18 — Use of privileged utility programs — Candidate evidence — assessor review

Restrict and tightly control the use of utility programs capable of overriding system and application controls.

A.8.19 — Installation of software on operational systems — Partially implemented (exception)

Implement procedures and measures to securely manage the installation of software on operational systems; software allowlisting, controlled deployment, change control.

A.8.20 — Networks security — Candidate evidence — assessor review

Secure, manage and control networks and network devices to protect information in systems and applications; firewalls, network security controls, segmentation.

A.8.21 — Security of network services — Candidate evidence — assessor review

Identify, implement and monitor security mechanisms, service levels and requirements for network services in service agreements.

A.8.22 — Segregation of networks — Manual assessment required

Segregate groups of information services, users and systems in networks to contain compromise and limit lateral movement; segmentation, VLANs, zoning.

A.8.23 — Web filtering — Partially implemented (exception)

Manage access to external websites to reduce exposure to malicious content; web filtering, secure web gateway, blocking of phishing and malware sites.

A.8.24 — Use of cryptography — Manual assessment required

Define and implement rules for effective use of cryptography including key management; encryption at rest and in transit, TLS, key lifecycle management.

A.8.25 — Secure development life cycle — Candidate evidence — assessor review

Establish and apply rules for the secure development of software and systems across the lifecycle; secure SDLC, security by design.

A.8.26 — Application security requirements — Candidate evidence — assessor review

Identify, specify and approve information security requirements when developing or acquiring applications.

A.8.27 — Secure system architecture and engineering principles — Candidate evidence — assessor review

Establish, document, maintain and apply principles for engineering secure systems to all development activities; security by design, defence in depth.

A.8.28 — Secure coding — Candidate evidence — assessor review

Apply secure coding principles to software development to prevent common vulnerabilities such as injection and cross-site scripting; code review, SAST, input validation, secure coding standards.

A.8.29 — Security testing in development and acceptance — Candidate evidence — assessor review

Define and implement security testing across the development lifecycle and at acceptance; penetration testing, application security testing, DAST, stress testing, test results before deployment.

A.8.30 — Outsourced development — Candidate evidence — assessor review

Direct, monitor and review activities related to outsourced system development so external developers meet the organisation's security standards.

A.8.31 — Separation of development, test and production environments — Candidate evidence — assessor review

Separate and secure development, test and production environments to prevent unauthorised change and protect production data; environment isolation.

A.8.32 — Change management — Candidate evidence — assessor review

Subject changes to information processing facilities and systems to change management procedures; assessment, authorisation, testing, approval, minimal disruption, CAB.

A.8.33 — Test information — Candidate evidence — assessor review

Select, protect and manage test information appropriately, avoiding use of live sensitive data or PII unless masked or sanitised.

A.8.34 — Protection of information systems during audit testing — Insufficient evidence

Plan and agree audit tests and assurance activities involving operational systems to minimise disruption and prevent accidental compromise.

5. Nonconformities (major/minor)

The exceptions below carry the engine's own severity, derived from the assessed state and the evidence behind it. Classifying a nonconformity as MAJOR or MINOR under ISO/IEC 27001 is the auditor's determination — it turns on whether the management system as a whole fails to meet a requirement — and is recorded by the assessor against these rows before issue.

#	Control	Area	Nature of exception	Result	Severity
E-1	A.8.1	User endpoint devices	User endpoint devices — touched by the evidence assessed against it (5 cited documents) but not established by it. (evidence route: uploaded evidence)	Partially implemented (exception)	Medium
E-2	A.8.2	Privileged access rights	Privileged access rights — touched by the evidence assessed against it (5 cited documents) but not established by it. (evidence route: uploaded evidence)	Partially implemented (exception)	Medium
E-3	A.8.9	Configuration management	Configuration management — touched by the evidence assessed against it (5 cited documents) but not established by it. (evidence route: uploaded evidence)	Partially implemented (exception)	Medium

#	Control	Area	Nature of exception	Result	Severity
E-4	A.8.12	Data leakage prevention	Data leakage prevention — touched by the evidence assessed against it (1 cited document) but not established by it. (evidence route: uploaded evidence)	Partially implemented (exception)	Medium
E-5	A.8.13	Information backup	Information backup — touched by the evidence assessed against it (1 cited document) but not established by it. (evidence route: uploaded evidence)	Partially implemented (exception)	Medium
E-6	A.8.16	Monitoring activities	Monitoring activities — touched by the evidence assessed against it (3 cited documents) but not established by it. (evidence route: uploaded evidence)	Partially implemented (exception)	Medium
E-7	A.8.19	Installation of software on operational systems	Installation of software on operational systems — touched by the evidence assessed against it (5 cited documents) but not established by it. (evidence route: uploaded evidence)	Partially implemented (exception)	Medium
E-8	A.8.23	Web filtering	Web filtering — touched by the evidence assessed against it (5 cited documents) but not established by it. (evidence route: uploaded evidence)	Partially implemented (exception)	Medium

How to read this table: each row is one adverse finding (an exception). Severity is High for a failed control, Medium for a partially met control; the assessor confirms severity before external issue. The exception numbers (E-n) are referenced by the remediation plan.

6. Corrective action plan

Phase	Actions	Start	Target	Milestone
Phase 2 — Complete partially met controls	8	2026-12-09	2027-02-07	Phase 2 complete: every action re-validated

How to read this table: the plan runs in phases from the report date: controls not met first, then partially met. Owners below are SUGGESTED ROLES taken from each control's own area; name the accountable person for each before work starts. The full plan, with every action, is in Remediation_Project_Plan.csv, which opens in Excel and imports into Microsoft Project.

Priority	Exception	Control	Recommended action	Suggested owner (role)	Target	Re-test
P2	E-1	A.8.1	Partially met — close the gap in User endpoint devices. Evidence that will close it: access control record, endpoint configuration, key management record, procedure document.	IT security operations lead	2027-02-07	Evidence re-validation
P2	E-2	A.8.2	Partially met — close the gap in Privileged access rights. Evidence that will close it: access control record, privileged access record, review record.	Identity and access lead	2027-02-07	Evidence re-validation
P2	E-3	A.8.9	Partially met — close the gap in Configuration management. Evidence that will close it: monitoring record, network diagram, review record, technical configuration.	IT security operations lead	2027-02-07	Evidence re-validation
P2	E-4	A.8.12	Partially met — close the gap in Data leakage prevention. Evidence that will close it: endpoint configuration, network diagram, technical configuration.	Information security manager	2027-02-07	Evidence re-validation
P2	E-5	A.8.13	Partially met — close the gap in Information backup. Evidence that will close it: backup record, policy document, restore test record.	Incident and continuity lead	2027-02-07	Evidence re-validation
P2	E-6	A.8.16	Partially met — close the gap in Monitoring activities. Evidence that will close it: assessment record, incident record, monitoring record, network diagram.	IT security operations lead	2027-02-07	Evidence re-validation
P2	E-7	A.8.19	Partially met — close the gap in Installation of software on operational systems. Evidence that will close it: procedure document, review record, technical configuration.	Engineering lead	2027-02-07	Evidence re-validation

Priority	Exception	Control	Recommended action	Suggested owner (role)	Target	Re-test
P2	E-8	A.8.23	Partially met — close the gap in Web filtering. Evidence that will close it: access control record, endpoint configuration, firewall rule review.	Information security manager	2027-02-07	Evidence re-validation

How to read this table: actions are ordered by priority — P1 rows (failed controls) first, then P2 (partially met). Each action names the control's own requirement and the evidence the canonical pack expects will close it. The owner is a suggested role and the target is the end of the action's phase; the accountable manager confirms both. Each action closes by re-submitting evidence for re-validation.

6a. Evidence-request and remediation register (fast-track)

8 controls to remediate · 81 for the assessor to confirm (candidate evidence on file) · 9 to request from the client · 18 insufficient evidence — the same assessed controls reported throughout this report, grouped into the assessor's working lists.

Pillar	Action	Control	Label	Result
Organizational	Assessor to confirm	A.5.1	Policies for information security	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.2	Information security roles and responsibilities	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.3	Segregation of duties	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.4	Management responsibilities	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.6	Contact with special interest groups	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.10	Acceptable use of information and other associated assets	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.13	Labelling of information	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.14	Information transfer	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.15	Access control	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.16	Identity management	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.17	Authentication information	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.18	Access rights	Candidate evidence — assessor review

Pillar	Action	Control	Label	Result
Organizational	Assessor to confirm	A.5.20	Addressing information security within supplier agreements	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.22	Monitoring, review and change management of supplier services	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.23	Information security for use of cloud services	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.24	Information security incident management planning and preparation	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.25	Assessment and decision on information security events	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.26	Response to information security incidents	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.28	Collection of evidence	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.29	Information security during disruption	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.30	ICT readiness for business continuity	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.33	Protection of records	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.34	Privacy and protection of PII	Candidate evidence — assessor review
Organizational	Assessor to confirm	A.5.37	Documented operating procedures	Candidate evidence — assessor review
Organizational	Request from client	A.5.11	Return of assets	Manual assessment required
Organizational	Re-evidence	A.5.5	Contact with authorities	Insufficient evidence
Organizational	Re-evidence	A.5.7	Threat intelligence	Insufficient evidence
Organizational	Re-evidence	A.5.8	Information security in project management	Insufficient evidence
Organizational	Re-evidence	A.5.9	Inventory of information and other associated assets	Insufficient evidence
Organizational	Re-evidence	A.5.12	Classification of information	Insufficient evidence
Organizational	Re-evidence	A.5.19	Information security in supplier relationships	Insufficient evidence

Pillar	Action	Control	Label	Result
Organizational	Re-evidence	A.5.21	Managing information security in the ICT supply chain	Insufficient evidence
Organizational	Re-evidence	A.5.27	Learning from information security incidents	Insufficient evidence
Organizational	Re-evidence	A.5.31	Legal, statutory, regulatory and contractual requirements	Insufficient evidence
Organizational	Re-evidence	A.5.32	Intellectual property rights	Insufficient evidence
Organizational	Re-evidence	A.5.35	Independent review of information security	Insufficient evidence
Organizational	Re-evidence	A.5.36	Compliance with policies, rules and standards for information security	Insufficient evidence
People	Assessor to confirm	A.6.1	Screening	Candidate evidence — assessor review
People	Assessor to confirm	A.6.2	Terms and conditions of employment	Candidate evidence — assessor review
People	Assessor to confirm	A.6.3	Information security awareness, education and training	Candidate evidence — assessor review
People	Assessor to confirm	A.6.4	Disciplinary process	Candidate evidence — assessor review
People	Assessor to confirm	A.6.5	Responsibilities after termination or change of employment	Candidate evidence — assessor review
People	Assessor to confirm	A.6.7	Remote working	Candidate evidence — assessor review
People	Request from client	A.6.6	Confidentiality or non-disclosure agreements	Manual assessment required
People	Re-evidence	A.6.8	Information security event reporting	Insufficient evidence
Physical	Assessor to confirm	A.7.1	Physical security perimeters	Candidate evidence — assessor review
Physical	Assessor to confirm	A.7.2	Physical entry	Candidate evidence — assessor review
Physical	Assessor to confirm	A.7.4	Physical security monitoring	Candidate evidence — assessor review
Physical	Assessor to confirm	A.7.5	Protecting against physical and environmental threats	Candidate evidence — assessor review
Physical	Assessor to confirm	A.7.6	Working in secure areas	Candidate evidence — assessor review

Pillar	Action	Control	Label	Result
Physical	Assessor to confirm	A.7.7	Clear desk and clear screen	Candidate evidence — assessor review
Physical	Assessor to confirm	A.7.9	Security of assets off-premises	Candidate evidence — assessor review
Physical	Assessor to confirm	A.7.11	Supporting utilities	Candidate evidence — assessor review
Physical	Assessor to confirm	A.7.12	Cabling security	Candidate evidence — assessor review
Physical	Assessor to confirm	A.7.13	Equipment maintenance	Candidate evidence — assessor review
Physical	Assessor to confirm	A.7.14	Secure disposal or re-use of equipment	Candidate evidence — assessor review
Physical	Re-evidence	A.7.3	Securing offices, rooms and facilities	Insufficient evidence
Physical	Re-evidence	A.7.8	Equipment siting and protection	Insufficient evidence
Physical	Re-evidence	A.7.10	Storage media	Insufficient evidence
Technological	Remediate	A.8.1	User endpoint devices	Partially implemented (exception)
Technological	Remediate	A.8.2	Privileged access rights	Partially implemented (exception)
Technological	Remediate	A.8.9	Configuration management	Partially implemented (exception)
Technological	Remediate	A.8.12	Data leakage prevention	Partially implemented (exception)
Technological	Remediate	A.8.13	Information backup	Partially implemented (exception)
Technological	Remediate	A.8.16	Monitoring activities	Partially implemented (exception)
Technological	Remediate	A.8.19	Installation of software on operational systems	Partially implemented (exception)
Technological	Remediate	A.8.23	Web filtering	Partially implemented (exception)
Technological	Assessor to confirm	A.8.3	Information access restriction	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.4	Access to source code	Candidate evidence — assessor review

Pillar	Action	Control	Label	Result
Technological	Assessor to confirm	A.8.5	Secure authentication	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.6	Capacity management	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.7	Protection against malware	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.10	Information deletion	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.11	Data masking	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.14	Redundancy of information processing facilities	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.15	Logging	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.17	Clock synchronisation	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.18	Use of privileged utility programs	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.20	Networks security	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.21	Security of network services	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.25	Secure development life cycle	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.26	Application security requirements	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.27	Secure system architecture and engineering principles	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.28	Secure coding	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.29	Security testing in development and acceptance	Candidate evidence — assessor review

Pillar	Action	Control	Label	Result
Technological	Assessor to confirm	A.8.30	Outsourced development	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.31	Separation of development, test and production environments	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.32	Change management	Candidate evidence — assessor review
Technological	Assessor to confirm	A.8.33	Test information	Candidate evidence — assessor review
Technological	Request from client	A.8.22	Segregation of networks	Manual assessment required
Technological	Request from client	A.8.24	Use of cryptography	Manual assessment required
Technological	Re-evidence	A.8.8	Management of technical vulnerabilities	Insufficient evidence
Technological	Re-evidence	A.8.34	Protection of information systems during audit testing	Insufficient evidence
Management system (clauses 4–10)	Assessor to confirm	4.4	Information security management system	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	5.1	Leadership and commitment	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	5.2	Policy	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	5.3	Organisational roles, responsibilities and authorities	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	6.1	Actions to address risks and opportunities	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	6.2	Information security objectives and planning	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	6.3	Planning of changes	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	7.2	Competence	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	7.3	Awareness	Candidate evidence — assessor review

Pillar	Action	Control	Label	Result
Management system (clauses 4–10)	Assessor to confirm	7.4	Communication	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	7.5	Documented information	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	8.1	Operational planning and control	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	8.2	Information security risk assessment	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	8.3	Information security risk treatment	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	9.1	Monitoring, measurement, analysis and evaluation	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	9.2	Internal audit	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	9.3	Management review	Candidate evidence — assessor review
Management system (clauses 4–10)	Assessor to confirm	10.2	Nonconformity and corrective action	Candidate evidence — assessor review
Management system (clauses 4–10)	Request from client	4.1	Understanding the organisation and its context	Manual assessment required
Management system (clauses 4–10)	Request from client	4.2	Needs and expectations of interested parties	Manual assessment required
Management system (clauses 4–10)	Request from client	4.3	Determining the scope of the ISMS	Manual assessment required
Management system (clauses 4–10)	Request from client	7.1	Resources	Manual assessment required
Management system (clauses 4–10)	Request from client	10.1	Continual improvement	Manual assessment required

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.

7. Risk assessment & treatment linkage

This section carries the residual position this assessment derived from its own control states, per domain, together with the adverse controls that drive each rating — which is the linkage the heading names, resolvable inside this document against the control assessment. Clauses 6.1.2, 6.1.3, 8.2 and 8.3 are themselves assessed, with cited evidence, in the management-system clauses section. The ISMS risk assessment and the risk treatment plan those clauses require are the organisation's own records; CyberSentien issues the risk assessment register and the risk treatment plan as the companion artefacts named on the report-format page.

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
Technological	34	0	0	8	26	Medium — default, assessor to confirm	A.8.1, A.8.2, A.8.3, A.8.4, A.8.5, A.8.6, A.8.7, A.8.8
Organizational	37	0	0	0	37	To be determined — default, assessor to confirm	A.5.1, A.5.2, A.5.3, A.5.4, A.5.5, A.5.6, A.5.7, A.5.8
People	8	0	0	0	8	To be determined — default, assessor to confirm	A.6.1, A.6.2, A.6.3, A.6.4, A.6.5, A.6.6, A.6.7, A.6.8
Physical	14	0	0	0	14	To be determined — default, assessor to confirm	A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6, A.7.7, A.7.8
Management system (clauses 4–10)	23	0	0	0	23	To be determined — default, assessor to confirm	4.1, 4.2, 4.3, 4.4, 5.1, 5.2, 5.3, 6.1

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.

7a. 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	A.8.5, A.5.15, A.5.17	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, CyberSentien HITRUST CSF Readiness Assessment, ISM / IRAP SAR
conditional access	A.8.5, A.5.15, A.8.3	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0
privileged roles	A.8.2, A.5.15, A.5.18	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0
guest accounts	A.5.16, A.5.15, A.5.18	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, NIST CSF 2.0, PCI DSS v4.0.1
dormant accounts	A.5.18, A.5.15, A.5.16	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0
network segmentation	A.8.22	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, NIST CSF 2.0, PCI DSS v4.0.1
firewall policy	A.8.20	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, NIST CSF 2.0, PCI DSS v4.0.1
transport encryption	A.8.24	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, NIST CSF 2.0, PCI DSS v4.0.1

Evidence signal	This framework	Also evidences (other frameworks)
network exposure	A.8.20	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, NIST CSF 2.0, PCI DSS v4.0.1
backup execution	A.8.13	APRA CPS 230 (Operational Risk), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0
restore testing	A.8.13	APRA CPS 230 (Operational Risk), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0
secure development	A.8.25, A.8.28	CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, NIST SP 800-53 Rev 5, CyberSentien Secure SDLC Assurance
central logging	A.8.15, A.8.16, A.5.7	APRA CPS 230 (Operational Risk), APRA CPS 234 (Information Security), Breach Reporting (OAIC NDB / CPS 234), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight
os patching	A.8.8, A.8.19, A.8.32	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0
app patching	A.8.8, A.8.19, A.8.32	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0, PCI DSS v4.0.1
vulnerability exposure	A.8.8, A.8.19	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, EU AI Act (Regulation 2024/1689), ISM / IRAP SAR
dlp	A.8.12, A.8.10, A.8.11	APRA CPS 234 (Information Security), Breach Reporting (OAIC NDB / CPS 234), CIS Controls v8, ISM / IRAP SAR, NIST SP 800-53 Rev 5, NIST CSF 2.0
retention	A.5.33, A.8.10	APRA CPS 234 (Information Security), 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
sensitivity labels	A.5.12, A.5.13	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, NIST SP 800-53 Rev 5, NIST CSF 2.0
ediscovery	A.5.28	NIST SP 800-53 Rev 5
acceptable use	A.5.10	CyberSentien CISSP-aligned Security Practice Assessment, Australian Early Childhood (ECEC — National Law, privacy & child safety), ISM / IRAP SAR, NIST SP 800-53 Rev 5
auth methods	A.8.5, A.5.15, A.5.17	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0, PCI DSS v4.0.1
security defaults	A.5.15	APRA CPS 234 (Information Security), CIS Controls v8, ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0, PCI DSS v4.0.1
application control	A.8.19, A.8.32, A.5.23	APRA CPS 234 (Information Security), CIS Controls v8, ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0, PCI DSS v4.0.1
device inventory	A.5.9, A.8.1	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, Australian Early Childhood (ECEC — National Law, privacy & child safety), ASD Essential Eight, ISM / IRAP SAR
device compliance	A.8.1, A.8.9	CIS Controls v8, Australian Early Childhood (ECEC — National Law, privacy & child safety), ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0, PCI DSS v4.0.1
device encryption	A.8.24	APRA CPS 234 (Information Security), Australian Early Childhood (ECEC — National Law, privacy & child safety), ISM / IRAP SAR, Australian Schools (cyber, privacy & child safety)
incident response	A.5.24, A.5.26	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, Australian Early Childhood (ECEC — National Law, privacy & child safety), ISM / IRAP SAR, NIST SP 800-53 Rev 5

Evidence signal	This framework	Also evidences (other frameworks)
security awareness	A.6.3	AU Gov — Responsible Use of AI, CIS Controls v8, Fraud & AML (AUSTRAC AML/CTF), ISM / IRAP SAR, NIST SP 800-53 Rev 5, NIST CSF 2.0
service resilience	A.5.30	APRA CPS 230 (Operational Risk), ISM / IRAP SAR
access governance	A.5.18, A.5.16	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, Fraud & AML (AUSTRAC AML/CTF), ISM / IRAP SAR, NIST SP 800-53 Rev 5
email security	A.8.23, A.8.7	APRA CPS 234 (Information Security), Breach Reporting (OAIC NDB / CPS 234), CIS Controls v8, ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0
external collaboration	A.5.14, A.5.23	APRA CPS 234 (Information Security), SOC 1 (ISAE 3402 / SSAE 18), SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
data sharing	A.8.12, A.5.14, A.5.13	APRA CPS 234 (Information Security), SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
identity groups	A.5.16, A.5.15, A.5.18	APRA CPS 234 (Information Security), CIS Controls v8, NIST CSF 2.0, PCI DSS v4.0.1, SOC 1 (ISAE 3402 / SSAE 18), SOC 2 (Trust Services Criteria)
domain verification	A.8.9	APRA CPS 234 (Information Security), ISM / IRAP SAR, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
endpoint protection	A.8.7, A.8.1	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, CyberSentien HITRUST CSF Readiness Assessment, ISM / IRAP SAR
siem logging	A.8.16, A.5.7, A.8.15	APRA CPS 234 (Information Security), Breach Reporting (OAIC NDB / CPS 234), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, EU AI Act (Regulation 2024/1689)
mfa enforced all users	A.8.5	APRA CPS 234 (Information Security), ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
mfa enforced privileged	A.8.5, A.8.2	APRA CPS 234 (Information Security), ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
mfa phishing resistant privileged	A.8.5	ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0
mfa registration complete	A.5.17	NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
legacy auth blocked	A.8.5	APRA CPS 234 (Information Security), NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
global admin count bounded	A.8.2	APRA CPS 234 (Information Security), ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
privileged access standing minimised	A.8.2	ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
inactive unprivileged disabled	A.5.18	APRA CPS 234 (Information Security), ISM / IRAP SAR, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)
inactive privileged disabled	A.8.2	ASD Essential Eight, ISM / IRAP SAR, NIST CSF 2.0, SOC 2 (Trust Services Criteria), SOC 3 (Trust Services Criteria — general-use report)

8. Internal audit & management review

This section carries what the assessment can evidence toward internal audit and management review: the issuance quality gate, the evidence register with its integrity hashes, and the changes observed over the period. The internal audit programme itself, and the management review minutes and decisions required by clauses 9.2 and 9.3, are the organisation's own records and are supplied by it.

Gate check	Status	Detail
Control catalogue assessed	PASS	116 controls assessed
Evidence-led coverage present	PASS	8 of 116 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	external-issue approval not recorded

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.

8a. Evidence register

A sample of the cited evidence, stratified across every control family, with the control each item 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.

This register shows 200 of 380 cited items, sampled across all 5 control families and covering 62 of 107 controls with cited evidence. Every family is accounted for in the table beneath. The complete register is in the assessment record.

#	Control	Cited document	Provenance	Integrity (SHA-256)
1	A.5.1	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e980b10188f726e4e250bec6d8a40da3e43
2	A.6.1	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
3	A.7.1	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
4	A.8.1	050_secure_system_build_hardening_procedure.pdf	Uploaded evidence	cf44bbd2d2df29cc10a849fe5cc07dd00be0fa1734dcaddca36916afde4a504d
5	4.4	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e980b10188f726e4e250bec6d8a40da3e43
6	A.5.1	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37a7c48f4cb50b5c6c2d37211f2791a516
7	A.6.1	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6
8	A.7.1	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6
9	A.8.1	035_endpoint_protection_standard.pdf	Uploaded evidence	d0f5b621bd23929a0d9479955eeb57771537739dd106d233c8e0396e3759458b
10	4.4	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37a7c48f4cb50b5c6c2d37211f2791a516
11	A.5.1	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	4027f4cd46d73e3ce32e965c8a49a215e5e432bf08703655d804c28af27dc3b2
12	A.6.1	052_audit_findings_risk_treatment_register.pdf	Uploaded evidence	5cc25603c344aeeebeaab3ca11ecd9f9a02128575ef1e8e5c8536da2d21cd56f
13	A.7.2	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
14	A.8.1	017_secure_configuration_baseline_standard.pdf	Uploaded evidence	5fcfa220809211f659ae6f12dee3031e1b6d3f19fea1ee1f698a11e24ba11145
15	4.4	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	4027f4cd46d73e3ce32e965c8a49a215e5e432bf08703655d804c28af27dc3b2
16	A.5.1	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
17	A.6.2	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
18	A.7.2	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6
19	A.8.1	016_patch_management_standard.pdf	Uploaded evidence	7d5c195985fd1f0a813192da1b3269dd2ae892a1a95f2fed385908c7ade79e40
20	4.4	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9

#	Control	Cited document	Provenance	Integrity (SHA-256)
21	A.5.2	029_security_governance_committee_charter.pdf	Uploaded evidence	e59df87042d8710787d77651b1ea20bd7fa9e9a2d76f733608670d68b91b4a35
22	A.6.2	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6
23	A.7.2	1229_privileged_access_configuration_export_pam_platform.pdf	Uploaded evidence	31e96f8caef6f13a37efb43f0dac8dda728b1b138aa255d7cf04615262507441
24	A.8.1	221_endpoint_protection_console_export_payments_switch.pdf	Uploaded evidence	b7d7ab942d91e6e97d592f9fee8598b07c60cc558839e855247e3a21fa2bd831
25	5.1	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e980b10188f726e4e250bec6d8a40da3e43
26	A.5.2	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37a7c48f4cb50b5c6c2d37211f2791a516
27	A.6.3	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
28	A.7.2	1245_phishing_resistant_mfa_registration_coverage_export_all_users_q3_2026.pdf	Uploaded evidence	0a088243128a3de912a3de403c691352c41b3aeab93281cbdb38f35a4e4af6c5
29	A.8.2	1229_privileged_access_configuration_export_pam_platform.pdf	Uploaded evidence	31e96f8caef6f13a37efb43f0dac8dda728b1b138aa255d7cf04615262507441
30	5.1	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	4027f4cd46d73e3ce32e965c8a49a215e5e432bf08703655d804c28af27dc3b2
31	A.5.2	047_personal_information_handling_procedure.pdf	Uploaded evidence	dc109a6f6de6c8620153aec52f4c947b7d944d2eb0998e85f898eb9f086f3ca3
32	A.6.3	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6
33	A.7.3	023_data_classification_handling_standard.pdf	Uploaded evidence	056d78ec3f060b14840e6d03e256abafd58ff5517ea0602993989da373920172
34	A.8.2	1228_multi_factor_authentication_configuration_export_entra_id_tenant.pdf	Uploaded evidence	dd3b9d2f6e6a5c690e995cda6184e18f539852b936dc365013034a57b0aae331
35	5.1	025_network_security_policy.pdf	Uploaded evidence	99f3533716db31c5a8f949c9574163c525c4d3217d07ca0a43d00670823baebc
36	A.5.2	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e980b10188f726e4e250bec6d8a40da3e43
37	A.6.3	128_security_awareness_training_completion_report_q2_2026.pdf	Uploaded evidence	15697abedbeafaf40d086d43b7e4884d52305254950364a5d04d53e01c583fd9
38	A.7.4	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
39	A.8.2	221_endpoint_protection_console_export_payments_switch.pdf	Uploaded evidence	b7d7ab942d91e6e97d592f9fee8598b07c60cc558839e855247e3a21fa2bd831
40	5.1	002_access_control_policy.pdf	Uploaded evidence	b0d7557047740e19743dc4450ec30df6db69ae4d366742e28bbc043e912b8189
41	A.5.2	011_data_breach_response_procedure.pdf	Uploaded evidence	4bc5e0e094add1c8bd11f714951f91afccb8ae920e28b586ccbfc49b921601ba
42	A.6.3	218_security_awareness_training_completion_report_q3_2025.pdf	Uploaded evidence	440dd0e6d2e4be35b9fdf5012696ec11f15be90bf4b5d333f1ef42ce7bfb1b52
43	A.7.4	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6
44	A.8.2	131_endpoint_protection_console_export_internet_banking.pdf	Uploaded evidence	e850c4525d85e0de57c1134e1a6a1cc82c34d44452b22b1f2ede8da4d481ca54
45	5.1	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6
46	A.5.3	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
47	A.6.3	209_phishing_simulation_results_q3_2025.pdf	Uploaded evidence	517564d4904a1eb75410dd1b68b166d67c02cbbb12c91a54cf69d3394becd26e
48	A.7.4	1229_privileged_access_configuration_export_pam_platform.pdf	Uploaded evidence	31e96f8caef6f13a37efb43f0dac8dda728b1b138aa255d7cf04615262507441
49	A.8.2	1245_phishing_resistant_mfa_registration_coverage_export_all_users_q3_2026.pdf	Uploaded evidence	0a088243128a3de912a3de403c691352c41b3aeab93281cbdb38f35a4e4af6c5

#	Control	Cited document	Provenance	Integrity (SHA-256)
50	5.2	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e980b10188f726e4e250bec6d8a40da3e43
51	A.5.3	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6
52	A.6.4	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
53	A.7.4	1245_phishing_resistant_mfa_registration_coverage_export_all_users_q3_2026.pdf	Uploaded evidence	0a088243128a3de912a3de403c691352c41b3aeab93281cbdb38f35a4e4af6c5
54	A.8.3	221_endpoint_protection_console_export_payments_switch.pdf	Uploaded evidence	b7d7ab942d91e6e97d592f9fee8598b07c60cc558839e855247e3a21fa2bd831
55	5.2	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37a7c48f4cb50b5c6c2d37211f2791a516
56	A.5.3	053_security_testing_assurance_procedure.pdf	Uploaded evidence	62b4dd18699dada10d686903090f2d5fcd8d6c4dabbf592fb97aca9b27d79adb
57	A.6.4	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6
58	A.7.4	117_soc_monitoring_report_q2_2026.pdf	Uploaded evidence	06ca0cc7ca28d8a40cd52910d13b31e8fc50ffa231af7bccbf6bec614bab39e3
59	A.8.3	131_endpoint_protection_console_export_internet_banking.pdf	Uploaded evidence	e850c4525d85e0de57c1134e1a6a1cc82c34d44452b22b1f2ede8da4d481ca54
60	5.2	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	4027f4cd46d73e3ce32e965c8a49a215e5e432bf08703655d804c28af27dc3b2
61	A.5.4	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e980b10188f726e4e250bec6d8a40da3e43
62	A.6.4	016_patch_management_standard.pdf	Uploaded evidence	7d5c195985fd1f0a813192da1b3269dd2ae892a1a95f2fed385908c7ade79e40
63	A.7.5	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
64	A.8.3	1229_privileged_access_configuration_export_pam_platform.pdf	Uploaded evidence	31e96f8caef6f13a37efb43f0dac8dda728b1b138aa255d7cf04615262507441
65	5.2	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
66	A.5.4	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37a7c48f4cb50b5c6c2d37211f2791a516
67	A.6.5	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e980b10188f726e4e250bec6d8a40da3e43
68	A.7.5	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6
69	A.8.3	1228_multi_factor_authentication_configuration_export_entra_id_tenant.pdf	Uploaded evidence	dd3b9d2f6e6a5c690e995cda6184e18f539852b936dc365013034a57b0aae331
70	5.3	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e980b10188f726e4e250bec6d8a40da3e43
71	A.5.4	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	4027f4cd46d73e3ce32e965c8a49a215e5e432bf08703655d804c28af27dc3b2
72	A.6.5	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37a7c48f4cb50b5c6c2d37211f2791a516
73	A.7.6	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
74	A.8.3	1245_phishing_resistant_mfa_registration_coverage_export_all_users_q3_2026.pdf	Uploaded evidence	0a088243128a3de912a3de403c691352c41b3aeab93281cbdb38f35a4e4af6c5
75	5.3	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37a7c48f4cb50b5c6c2d37211f2791a516
76	A.5.4	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
77	A.6.5	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	4027f4cd46d73e3ce32e965c8a49a215e5e432bf08703655d804c28af27dc3b2
78	A.7.6	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6

#	Control	Cited document	Provenance	Integrity (SHA-256)
79	A.8.4	053_security_testing_assurance_procedure.pdf	Uploaded evidence	`62b4dd18699dada10d686903090f2d5f cd8d6c4dabbf592fb97aca9b27d79adb`
80	5.3	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	`4027f4cd46d73e3ce32e965c8a49a215 e5e432bf08703655d804c28af27dc3b2`
81	A.5.5	208_incident_post_mortem_q3_2025.pdf	Uploaded evidence	`72971ff13676a070d519006e11981d4f 404f7a93f71ad11bd0b16108e8cc9b51`
82	A.6.5	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	`463bd5f5a183a9e9c20ac5cb95bebec1 a734242cfc9c55a4aebfce108c4bf3f9`
83	A.7.7	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	`463bd5f5a183a9e9c20ac5cb95bebec1 a734242cfc9c55a4aebfce108c4bf3f9`
84	A.8.4	050_secure_system_build_hardening_procedure.pdf	Uploaded evidence	`cf44bbd2d2df29cc10a849fe5cc07dd0 0be0fa1734dcaddca36916afde4a504d`
85	5.3	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	`463bd5f5a183a9e9c20ac5cb95bebec1 a734242cfc9c55a4aebfce108c4bf3f9`
86	A.5.5	118_incident_post_mortem_q2_2026.pdf	Uploaded evidence	`ee3caab338c2fe87bc753c91d7620931 3be05224d77f638430814 21874d3084b`
87	A.6.7	046_records_management_data_handling_procedure.pdf	Uploaded evidence	`291c9ae746a67e3d6f0e7e28a53abe37 a7c48f4cb50b5c6c2d37211f2791a516`
88	A.7.7	041_physical_environmental_security_policy.pdf	Uploaded evidence	`d0fa967acaaf98dc3a04dd93f060ad53 7a98613b1b03971f2843e12a55df6ce6`
89	A.8.4	001_information_security_policy.pdf	Uploaded evidence	`19b799381535e5ed6e887320078e2e98 0b10188f726e4e250bec6d8a40da3e43`
90	6.1	046_records_management_data_handling_procedure.pdf	Uploaded evidence	`291c9ae746a67e3d6f0e7e28a53abe37 a7c48f4cb50b5c6c2d37211f2791a516`
91	A.5.6	029_security_governance_committee_charter.pdf	Uploaded evidence	`e59df87042d8710787d77651b1ea20bd 7fa9e9a2d76f733608670d68b91b4a35`
92	A.6.7	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	`4027f4cd46d73e3ce32e965c8a49a215 e5e432bf08703655d804c28af27dc3b2`
93	A.7.8	023_data_classification_handling_standard.pdf	Uploaded evidence	`056d78ec3f060b14840e6d03e256abaf d58ff5517ea0602993989da373920172`
94	A.8.4	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	`463bd5f5a183a9e9c20ac5cb95bebec1 a734242cfc9c55a4aebfce108c4bf3f9`
95	6.1	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	`463bd5f5a183a9e9c20ac5cb95bebec1 a734242cfc9c55a4aebfce108c4bf3f9`
96	A.5.6	046_records_management_data_handling_procedure.pdf	Uploaded evidence	`291c9ae746a67e3d6f0e7e28a53abe37 a7c48f4cb50b5c6c2d37211f2791a516`
97	A.6.7	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	`463bd5f5a183a9e9c20ac5cb95bebec1 a734242cfc9c55a4aebfce108c4bf3f9`
98	A.7.9	023_data_classification_handling_standard.pdf	Uploaded evidence	`056d78ec3f060b14840e6d03e256abaf d58ff5517ea0602993989da373920172`
99	A.8.5	053_security_testing_assurance_procedure.pdf	Uploaded evidence	`62b4dd18699dada10d686903090f2d5f cd8d6c4dabbf592fb97aca9b27d79adb`
100	6.1	011_data_breach_response_procedure.pdf	Uploaded evidence	`4bc5e0e094add1c8bd11f714951f91af ccb8ae920e28b586ccbfc49b921601ba`
101	A.5.6	011_data_breach_response_procedure.pdf	Uploaded evidence	`4bc5e0e094add1c8bd11f714951f91af ccb8ae920e28b586ccbfc49b921601ba`
102	A.6.7	011_data_breach_response_procedure.pdf	Uploaded evidence	`4bc5e0e094add1c8bd11f714951f91af ccb8ae920e28b586ccbfc49b921601ba`
103	A.7.10	023_data_classification_handling_standard.pdf	Uploaded evidence	`056d78ec3f060b14840e6d03e256abaf d58ff5517ea0602993989da373920172`
104	A.8.5	002_access_control_policy.pdf	Uploaded evidence	`b0d7557047740e19743dc4450ec30df6 db69ae4d366742e28bbc043e912b8189`
105	6.1	053_security_testing_assurance_procedure.pdf	Uploaded evidence	`62b4dd18699dada10d686903090f2d5f cd8d6c4dabbf592fb97aca9b27d79adb`
106	A.5.6	047_personal_information_handling_procedure.pdf	Uploaded evidence	`dc109a6f6de6c8620153aec52f4c947b 7d944d2eb0998e85f898eb9f086f3ca3`
107	A.6.8	008_logging_monitoring_policy.pdf	Uploaded evidence	`808a97e670d8c146b60deffd1db23c48 631586d78316946224c5e30f191f36ae`

#	Control	Cited document	Provenance	Integrity (SHA-256)
108	A.7.11	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
109	A.8.5	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e980b10188f726e4e250bec6d8a40da3e43
110	6.2	013_disaster_recovery_plan.pdf	Uploaded evidence	43e28b398d1d5644d3719a74fee67c20af34499386b572d0f34c6bf01675ad6e
111	A.5.6	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	4027f4cd46d73e3ce32e965c8a49a215e5e432bf08703655d804c28af27dc3b2
112	A.7.11	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6
113	A.8.5	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	4027f4cd46d73e3ce32e965c8a49a215e5e432bf08703655d804c28af27dc3b2
114	6.2	010_incident_response_plan.pdf	Uploaded evidence	42ae3973059050231da613b651b6b2ce0ac19f4ae2d69bb4d8a17abdbaae5d6b
115	A.5.7	052_audit_findings_risk_treatment_register.pdf	Uploaded evidence	5cc25603c344aeeebeaab3ca11ecd9f9a02128575ef1e8e5c8536da2d21cd56f
116	A.7.11	1228_multi_factor_authentication_configuration_export_entra_id_tenant.pdf	Uploaded evidence	dd3b9d2f6e6a5c690e995cda6184e18f539852b936dc365013034a57b0aae331
117	A.8.6	008_logging_monitoring_policy.pdf	Uploaded evidence	808a97e670d8c146b60deffd1db23c48631586d78316946224c5e30f191f36ae
118	6.3	010_incident_response_plan.pdf	Uploaded evidence	42ae3973059050231da613b651b6b2ce0ac19f4ae2d69bb4d8a17abdbaae5d6b
119	A.5.8	052_audit_findings_risk_treatment_register.pdf	Uploaded evidence	5cc25603c344aeeebeaab3ca11ecd9f9a02128575ef1e8e5c8536da2d21cd56f
120	A.7.11	1229_privileged_access_configuration_export_pam_platform.pdf	Uploaded evidence	31e96f8caef6f13a37efb43f0dac8dda728b1b138aa255d7cf04615262507441
121	A.8.6	1224_application_control_event_log_extract_workstations_q2_2026.pdf	Uploaded evidence	d8c9185aed6732269e88bc04e603af3abff3d2267a3d20c34a147dfd477f65bb
122	6.3	013_disaster_recovery_plan.pdf	Uploaded evidence	43e28b398d1d5644d3719a74fee67c20af34499386b572d0f34c6bf01675ad6e
123	A.5.9	104_vulnerability_scan_report_core_banking_temenos_t24_q2_2026.pdf	Uploaded evidence	57d272bb1f0ca21a99285efb37ed16d6b1176c057d8a4802072a3e6d81ccc75f
124	A.7.12	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
125	A.8.6	117_soc_monitoring_report_q2_2026.pdf	Uploaded evidence	06ca0cc7ca28d8a40cd52910d13b31e8fc50ffa231af7bccbf6bec614bab39e3
126	7.2	128_security_awareness_training_completion_report_q2_2026.pdf	Uploaded evidence	15697abedbeafaf40d086d43b7e4884d52305254950364a5d04d53e01c583fd9
127	A.5.9	112_patch_compliance_report_core_banking_temenos_t24_q2_2026.pdf	Uploaded evidence	159ccb7ae03586d8751c6cef5334f856b107f8844678e78d8733e94602e44a2d
128	A.7.12	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6
129	A.8.6	207_soc_monitoring_report_q3_2025.pdf	Uploaded evidence	bace47f7be25ed0aa0ce34dabebae7a4fc45755ae7421c6261eb1247ca2c9161
130	7.2	218_security_awareness_training_completion_report_q3_2025.pdf	Uploaded evidence	440dd0e6d2e4be35b9fdf5012696ec11f15be90bf4b5d333f1ef42ce7bfb1b52
131	A.5.9	202_patch_compliance_report_core_banking_temenos_t24_q3_2025.pdf	Uploaded evidence	54433d09b73075c7b2b80089e8c267dd975452e29be2199b39f7846a419c8d8e
132	A.7.13	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
133	A.8.7	1240_powershell_and_process_creation_auditing_configuration_export_windows_fleet.pdf	Uploaded evidence	9e603bbcafff9a0bce830d4398701618ff146a6aded42a8f44461a1741d54b91
134	7.2	209_phishing_simulation_results_q3_2025.pdf	Uploaded evidence	517564d4904a1eb75410dd1b68b166d67c02cbbb12c91a54cf69d3394becd26e
135	A.5.10	023_data_classification_handling_standard.pdf	Uploaded evidence	056d78ec3f060b14840e6d03e256abafd58ff5517ea0602993989da373920172
136	A.7.13	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6

#	Control	Cited document	Provenance	Integrity (SHA-256)
137	A.8.7	1226_browser_and_pdf_reader_hardening_configuration_export_workstations.pdf	Uploaded evidence	59c5e77d31b927324b2434dbe6cbd3cb03d30276911e965998d668e61fb1861b
138	7.2	119_phishing_simulation_results_q2_2026.pdf	Uploaded evidence	cffc8be96d1995348f9ed98417ffce04cd189d58955e90d40ece4b0312816dc3
139	A.5.10	1228_multi_factor_authentication_configuration_export_entra_id_tenant.pdf	Uploaded evidence	dd3b9d2f6e6a5c690e995cda6184e18f539852b936dc365013034a57b0aae331
140	A.7.14	023_data_classification_handling_standard.pdf	Uploaded evidence	056d78ec3f060b14840e6d03e256abafd58ff5517ea0602993989da373920172
141	A.8.7	1235_wdac_application_control_policy_configuration_export_workstations_and_servers.pdf	Uploaded evidence	c128df5d52eab8b3bdadc61313429174ff1f5ecca747e5905df69d25b1005505
142	7.3	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6
143	A.5.10	1229_privileged_access_configuration_export_pam_platform.pdf	Uploaded evidence	31e96f8caef6f13a37efb43f0dac8dda728b1b138aa255d7cf04615262507441
144	A.8.7	1225_office_macro_configuration_export_microsoft_365_tenant.pdf	Uploaded evidence	7f96fad8ce291188f34bae933d3b3f518609432d35593a78d3d1e3b0c70c1633
145	7.3	016_patch_management_standard.pdf	Uploaded evidence	7d5c195985fd1f0a813192da1b3269dd2ae892a1a95f2fed385908c7ade79e40
146	A.5.10	1245_phishing_resistant_mfa_registration_coverage_export_all_users_q3_2026.pdf	Uploaded evidence	0a088243128a3de912a3de403c691352c41b3aeab93281cbdb38f35a4e4af6c5
147	A.8.7	222_secure_configuration_export_payments_switch.pdf	Uploaded evidence	6f971a57866af59dc4f35d97ad4ecea1fdb5553c750d8ce94e42660b59b6a7fd
148	7.3	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
149	A.5.12	023_data_classification_handling_standard.pdf	Uploaded evidence	056d78ec3f060b14840e6d03e256abafd58ff5517ea0602993989da373920172
150	A.8.8	104_vulnerability_scan_report_core_banking_temenos_t24_q2_2026.pdf	Uploaded evidence	57d272bb1f0ca21a99285efb37ed16d6b1176c057d8a4802072a3e6d81ccc75f
151	7.3	128_security_awareness_training_completion_report_q2_2026.pdf	Uploaded evidence	15697abedbeafaf40d086d43b7e4884d52305254950364a5d04d53e01c583fd9
152	A.5.13	023_data_classification_handling_standard.pdf	Uploaded evidence	056d78ec3f060b14840e6d03e256abafd58ff5517ea0602993989da373920172
153	A.8.8	112_patch_compliance_report_core_banking_temenos_t24_q2_2026.pdf	Uploaded evidence	159ccb7ae03586d8751c6cef5334f856b107f8844678e78d8733e94602e44a2d
154	7.3	218_security_awareness_training_completion_report_q3_2025.pdf	Uploaded evidence	440dd0e6d2e4be35b9fdf5012696ec11f15be90bf4b5d333f1ef42ce7bfb1b52
155	A.5.14	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37a7c48f4cb50b5c6c2d37211f2791a516
156	A.8.8	202_patch_compliance_report_core_banking_temenos_t24_q3_2025.pdf	Uploaded evidence	54433d09b73075c7b2b80089e8c267dd975452e29be2199b39f7846a419c8d8e
157	7.4	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37a7c48f4cb50b5c6c2d37211f2791a516
158	A.5.14	047_personal_information_handling_procedure.pdf	Uploaded evidence	dc109a6f6de6c8620153aec52f4c947b7d944d2eb0998e85f898eb9f086f3ca3
159	A.8.8	008_logging_monitoring_policy.pdf	Uploaded evidence	808a97e670d8c146b60deffd1db23c48631586d78316946224c5e30f191f36ae
160	7.4	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
161	A.5.15	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
162	A.8.8	209_phishing_simulation_results_q3_2025.pdf	Uploaded evidence	517564d4904a1eb75410dd1b68b166d67c02cbbb12c91a54cf69d3394becd26e
163	7.4	011_data_breach_response_procedure.pdf	Uploaded evidence	4bc5e0e094add1c8bd11f714951f91afccb8ae920e28b586ccbfc49b921601ba
164	A.5.15	002_access_control_policy.pdf	Uploaded evidence	b0d7557047740e19743dc4450ec30df6db69ae4d366742e28bbc043e912b8189
165	A.8.9	221_endpoint_protection_console_export_payments_switch.pdf	Uploaded evidence	b7d7ab942d91e6e97d592f9fee8598b07c60cc558839e855247e3a21fa2bd831

#	Control	Cited document	Provenance	Integrity (SHA-256)
166	7.4	053_security_testing_assurance_procedure.pdf	Uploaded evidence	62b4dd18699dada10d686903090f2d5f cd8d6c4dabbf592fb97aca9b27d79adb
167	A.5.15	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad53 7a98613b1b03971f2843e12a55df6ce6
168	A.8.9	131_endpoint_protection_console_export_internet_banking.pdf	Uploaded evidence	e850c4525d85e0de57c1134e1a6a1cc8 2c34d44452b22b1f2ede8da4d481ca54
169	7.5	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e98 0b10188f726e4e250bec6d8a40da3e43
170	A.5.15	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37 a7c48f4cb50b5c6c2d37211f2791a516
171	A.8.9	1240_powershell_and_process_creation_auditing_configuration_export_windows_fleet.pdf	Uploaded evidence	9e603bbcafff9a0bce830d4398701618 ff146a6aded42a8f44461a1741d54b91
172	7.5	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37 a7c48f4cb50b5c6c2d37211f2791a516
173	A.5.16	221_endpoint_protection_console_export_payments_switch.pdf	Uploaded evidence	b7d7ab942d91e6e97d592f9fee8598b0 7c60cc558839e855247e3a21fa2bd831
174	A.8.9	1235_wdac_application_control_policy_configuration_export_workstations_and_servers.pdf	Uploaded evidence	c128df5d52eab8b3bdadc61313429174 ff1f5ecca747e5905df69d25b1005505
175	7.5	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	4027f4cd46d73e3ce32e965c8a49a215 e5e432bf08703655d804c28af27dc3b2
176	A.5.16	131_endpoint_protection_console_export_internet_banking.pdf	Uploaded evidence	e850c4525d85e0de57c1134e1a6a1cc8 2c34d44452b22b1f2ede8da4d481ca54
177	A.8.9	222_secure_configuration_export_payments_switch.pdf	Uploaded evidence	6f971a57866af59dc4f35d97ad4ecea1 fdb5553c750d8ce94e42660b59b6a7fd
178	7.5	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1 a734242cfc9c55a4aebfce108c4bf3f9
179	A.5.16	1228_multi_factor_authentication_configuration_export_entra_id_tenant.pdf	Uploaded evidence	dd3b9d2f6e6a5c690e995cda6184e18f 539852b936dc365013034a57b0aae331
180	A.8.10	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37 a7c48f4cb50b5c6c2d37211f2791a516
181	8.1	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37 a7c48f4cb50b5c6c2d37211f2791a516
182	A.5.16	1229_privileged_access_configuration_export_pam_platform.pdf	Uploaded evidence	31e96f8caef6f13a37efb43f0dac8dda 728b1b138aa255d7cf04615262507441
183	A.8.10	047_personal_information_handling_procedure.pdf	Uploaded evidence	dc109a6f6de6c8620153aec52f4c947b 7d944d2eb0998e85f898eb9f086f3ca3
184	8.1	047_personal_information_handling_procedure.pdf	Uploaded evidence	dc109a6f6de6c8620153aec52f4c947b 7d944d2eb0998e85f898eb9f086f3ca3
185	A.5.16	1245_phishing_resistant_mfa_registration_coverage_export_all_users_q3_2026.pdf	Uploaded evidence	0a088243128a3de912a3de403c691352 c41b3aeab93281cbdb38f35a4e4af6c5
186	A.8.10	011_data_breach_response_procedure.pdf	Uploaded evidence	4bc5e0e094add1c8bd11f714951f91af ccb8ae920e28b586ccbfc49b921601ba
187	8.1	052_audit_findings_risk_treatment_register.pdf	Uploaded evidence	5cc25603c344aeeebeaab3ca11ecd9f9 a02128575ef1e8e5c8536da2d21cd56f
188	A.5.17	002_access_control_policy.pdf	Uploaded evidence	b0d7557047740e19743dc4450ec30df6 db69ae4d366742e28bbc043e912b8189
189	A.8.10	022_privacy_policy.pdf	Uploaded evidence	e9579dc88cc528afc98aa8e1d6f67d6e 6539bbd161118cbab80be44c4ce0a362
190	8.2	037_security_awareness_training_policy.pdf	Uploaded evidence	3da7a066b10e4b33175bd00c5b70162a da5d4734a6b5ebe02089c2f6f4805816
191	A.5.17	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e98 0b10188f726e4e250bec6d8a40da3e43
192	A.8.10	038_data_retention_disposal_standard.pdf	Uploaded evidence	7763782c1a385bad780515fde9aade2c 7a5484acb2a6ff8b12c85a4e0742d3c1
193	8.2	052_audit_findings_risk_treatment_register.pdf	Uploaded evidence	5cc25603c344aeeebeaab3ca11ecd9f9 a02128575ef1e8e5c8536da2d21cd56f
194	A.5.17	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	4027f4cd46d73e3ce32e965c8a49a215 e5e432bf08703655d804c28af27dc3b2

#	Control	Cited document	Provenance	Integrity (SHA-256)
195	A.8.11	022_privacy_policy.pdf	Uploaded evidence	e9579dc88cc528afc98aa8e1d6f67d6e6539bbd161118cbab80be44c4ce0a362
196	8.3	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37a7c48f4cb50b5c6c2d37211f2791a516
197	A.5.17	025_network_security_policy.pdf	Uploaded evidence	99f3533716db31c5a8f949c9574163c525c4d3217d07ca0a43d00670823baebc
198	A.8.11	038_data_retention_disposal_standard.pdf	Uploaded evidence	7763782c1a385bad780515fde9aade2c7a5484acb2a6ff8b12c85a4e0742d3c1
199	8.3	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9
200	A.5.17	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6

How the counts relate. This register has one row per control–document citation: 380 citations of 57 distinct documents across 107 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.

8aa. Cited evidence by control family (complete — every family, including those with no row printed above)

Control family	Controls with cited evidence	Cited items	Distinct documents	Rows printed above
Organizational	36	134	40	50
People	7	22	12	22
Physical	14	30	7	30
Technological	32	128	40	49
Management system (clauses 4–10)	18	66	23	49

8b. 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 116 assessed controls with its result, the 57 cited evidence documents by name and the 57 evidence SHA-256 hashes recorded for them.

Distinct evidence artefacts	57
Controls with cited evidence	107
Artefacts carrying a SHA-256 hash	57 of 57
Manifest hash (SHA-256)	325d250c14ddf7a89f15aabacf64b892e1e09a90c298c9a0d08f8bab28955988

8c. 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.

9. 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 57 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.

10. 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 ISO 27001 that test result is: at least 95% correct (4 wrong in 185 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.

11. ISO/IEC 27001:2022 certification readiness conclusion

Of 116 controls, 8 were assessed from evidence (0 implemented, 0% of those assessed). Outstanding: 8 partially implemented; 9 requiring assessor review — no signal or uploaded evidence; 81 candidate evidence — assessor review; 18 insufficient evidence. This is a CyberSentien ISMS assessment / certification-readiness report. It is NOT an ISO certification decision, which requires an accredited certification body to conduct a Stage 1 and Stage 2 audit and issue the certificate. Annex A controls are referenced by identifier and CyberSentien's own short labels — no copyrighted ISO text is reproduced.

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.

12. 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 · 35 Medium · 81 Low — 116 open controls in all.

Control	Risk	Why rated	Action	Suggested owner (role)	Target date
4.1	**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
4.2	**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
4.3	**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
7.1	**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
10.1	**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
A.5.5	**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
A.5.7	**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
A.5.8	**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
A.5.9	**Medium**	The evidence supplied does not establish the control	Supply operating records that show the control working during the period	IT security operations lead	2027-01-08
A.5.11	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	IT security operations lead	2027-01-08
A.5.12	**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
A.5.19	**Medium**	The evidence supplied does not establish the control	Supply operating records that show the control working during the period	Third-party risk owner	2027-01-08
A.5.21	**Medium**	The evidence supplied does not establish the control	Supply operating records that show the control working during the period	Third-party risk owner	2027-01-08
A.5.27	**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
A.5.31	**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
A.5.32	**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
A.5.35	**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
A.5.36	**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
A.6.6	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	People and security awareness lead	2027-01-08
A.6.8	**Medium**	The evidence supplied does not establish the control	Supply operating records that show the control working during the period	People and security awareness lead	2027-01-08
A.7.3	**Medium**	The evidence supplied does not establish the control	Supply operating records that show the control working during the period	Facilities and physical security manager	2027-01-08
A.7.8	**Medium**	The evidence supplied does not establish the control	Supply operating records that show the control working during the period	Facilities and physical security manager	2027-01-08
A.7.10	**Medium**	The evidence supplied does not establish the control	Supply operating records that show the control working during the period	Facilities and physical security manager	2027-01-08
A.8.1	**Medium**	Evidence supports the control only in part	Partially met — close the gap in User endpoint devices. Evidence that will close it: access control record, endpoint configuration, key management record, procedure document.	IT security operations lead	2027-01-08
A.8.2	**Medium**	Evidence supports the control only in part	Partially met — close the gap in Privileged access rights. Evidence that will close it: access control record, privileged access record, review record.	Identity and access lead	2027-01-08
A.8.8	**Medium**	The evidence supplied does not establish the control	Supply operating records that show the control working during the period	IT security operations lead	2027-01-08
A.8.9	**Medium**	Evidence supports the control only in part	Partially met — close the gap in Configuration management. Evidence that will close it: monitoring record, network diagram, review record, technical configuration.	IT security operations lead	2027-01-08
A.8.12	**Medium**	Evidence supports the control only in part	Partially met — close the gap in Data leakage prevention. Evidence that will close it: endpoint configuration, network diagram, technical configuration.	Information security manager	2027-01-08

Control	Risk	Why rated	Action	Suggested owner (role)	Target date
A.8.13	**Medium**	Evidence supports the control only in part	Partially met — close the gap in Information backup. Evidence that will close it: backup record, policy document, restore test record.	Incident and continuity lead	2027-01-08
A.8.16	**Medium**	Evidence supports the control only in part	Partially met — close the gap in Monitoring activities. Evidence that will close it: assessment record, incident record, monitoring record, network diagram.	IT security operations lead	2027-01-08
A.8.19	**Medium**	Evidence supports the control only in part	Partially met — close the gap in Installation of software on operational systems. Evidence that will close it: procedure document, review record, technical configuration.	Engineering lead	2027-01-08
A.8.22	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	IT security operations lead	2027-01-08
A.8.23	**Medium**	Evidence supports the control only in part	Partially met — close the gap in Web filtering. Evidence that will close it: access control record, endpoint configuration, firewall rule review.	Information security manager	2027-01-08
A.8.24	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	IT security operations lead	2027-01-08
A.8.34	**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
4.4	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
5.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
5.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
5.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Incident and continuity lead	2027-02-07
6.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
6.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
6.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
7.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
7.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	People and security awareness lead	2027-02-07
7.4	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
7.5	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
8.1	**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
8.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
8.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
9.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	IT security operations lead	2027-02-07
9.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
9.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
10.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.5.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.5.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Incident and continuity lead	2027-02-07
A.5.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.5.4	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Incident and continuity lead	2027-02-07
A.5.6	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.5.10	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	IT security operations lead	2027-02-07
A.5.13	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.5.14	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.5.15	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Identity and access lead	2027-02-07
A.5.16	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Identity and access lead	2027-02-07
A.5.17	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Identity and access lead	2027-02-07
A.5.18	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Identity and access lead	2027-02-07
A.5.20	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Third-party risk owner	2027-02-07
A.5.22	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Third-party risk owner	2027-02-07

Control	Risk	Why rated	Action	Suggested owner (role)	Target date
A.5.23	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	IT security operations lead	2027-02-07
A.5.24	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Incident and continuity lead	2027-02-07
A.5.25	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.5.26	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Incident and continuity lead	2027-02-07
A.5.28	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.5.29	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.5.30	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Incident and continuity lead	2027-02-07
A.5.33	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.5.34	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Privacy officer	2027-02-07
A.5.37	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.6.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	People and security awareness lead	2027-02-07
A.6.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	People and security awareness lead	2027-02-07
A.6.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	People and security awareness lead	2027-02-07
A.6.4	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	People and security awareness lead	2027-02-07
A.6.5	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Incident and continuity lead	2027-02-07
A.6.7	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	People and security awareness lead	2027-02-07
A.7.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Facilities and physical security manager	2027-02-07
A.7.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Facilities and physical security manager	2027-02-07
A.7.4	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Facilities and physical security manager	2027-02-07
A.7.5	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Facilities and physical security manager	2027-02-07

Control	Risk	Why rated	Action	Suggested owner (role)	Target date
A.7.6	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Facilities and physical security manager	2027-02-07
A.7.7	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Facilities and physical security manager	2027-02-07
A.7.9	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Facilities and physical security manager	2027-02-07
A.7.11	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Facilities and physical security manager	2027-02-07
A.7.12	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Facilities and physical security manager	2027-02-07
A.7.13	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Facilities and physical security manager	2027-02-07
A.7.14	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Facilities and physical security manager	2027-02-07
A.8.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Identity and access lead	2027-02-07
A.8.4	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Identity and access lead	2027-02-07
A.8.5	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Identity and access lead	2027-02-07
A.8.6	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.8.7	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	IT security operations lead	2027-02-07
A.8.10	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.8.11	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.8.14	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Facilities and physical security manager	2027-02-07
A.8.15	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	IT security operations lead	2027-02-07
A.8.17	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.8.18	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Identity and access lead	2027-02-07
A.8.20	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	IT security operations lead	2027-02-07
A.8.21	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	IT security operations lead	2027-02-07

Control	Risk	Why rated	Action	Suggested owner (role)	Target date
A.8.25	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Engineering lead	2027-02-07
A.8.26	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Engineering lead	2027-02-07
A.8.27	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.8.28	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
A.8.29	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Engineering lead	2027-02-07
A.8.30	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Third-party risk owner	2027-02-07
A.8.31	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Engineering lead	2027-02-07
A.8.32	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Engineering lead	2027-02-07
A.8.33	**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).

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
5.2	Policy	Close call: an assessor reviews the cited document first	A documented procedure; an approved policy
5.3	Organisational roles, responsibilities and authorities	Close call: an assessor reviews the cited document first	A governance record (minutes or a decision record); a documented procedure
7.2	Competence	Close call: an assessor reviews the cited document first	Training completion records
7.3	Awareness	Close call: an assessor reviews the cited document first	Training completion records; an approved policy
7.5	Documented information	Close call: an assessor reviews the cited document first	A governance record (minutes or a decision record); a documented procedure
8.1	Operational planning and control	Close call: an assessor reviews the cited document first	A risk assessment; an approved plan; a documented procedure
9.1	Monitoring, measurement, analysis and evaluation	Close call: an assessor reviews the cited document first	Monitoring records (alerts and their triage); an assessment record; a governance record (minutes or a decision record)
A.5.1	Policies for information security	Close call: an assessor reviews the cited document first	A signed review record; an approval record; a governance record (minutes or a decision record)
A.5.16	Identity management	Close call: an assessor reviews the cited document first	Access control records (user and role listings); a signed review record; a governance record (minutes or a decision record)
A.5.17	Authentication information	Close call: an assessor reviews the cited document first	Access control records (user and role listings); an approved policy
A.5.19	Information security in supplier relationships	Close call: an assessor reviews the cited document first	A risk assessment; supplier assurance reports; the relevant contract clauses
A.5.2	Information security roles and responsibilities	Close call: an assessor reviews the cited document first	A governance record (minutes or a decision record)
A.5.21	Managing information security in the ICT supply chain	Close call: an assessor reviews the cited document first	A risk assessment; supplier assurance reports
A.5.22	Monitoring, review and change management of supplier services	Close call: an assessor reviews the cited document first	Monitoring records (alerts and their triage); a signed review record; audit records
A.5.24	Information security incident management planning and preparation	Close call: an assessor reviews the cited document first	Incident records; a governance record (minutes or a decision record); an approved plan
A.5.26	Response to information security incidents	Close call: an assessor reviews the cited document first	Backup job records; incident records; a documented procedure
A.5.35	Independent review of information security	Close call: an assessor reviews the cited document first	A signed review record; audit records; an approved plan
A.5.36	Compliance with policies, rules and standards for information security	Close call: an assessor reviews the cited document first	A signed review record; audit records
A.5.37	Documented operating procedures	Close call: an assessor reviews the cited document first	A documented procedure
A.5.5	Contact with authorities	Close call: an assessor reviews the cited document first	Incident records; a governance record (minutes or a decision record)
A.6.3	Information security awareness, education and training	Close call: an assessor reviews the cited document first	Training completion records; a governance record (minutes or a decision record)
A.8.15	Logging	Close call: an assessor reviews the cited document first	A log extract; audit records
A.8.18	Use of privileged utility programs	Close call: an assessor reviews the cited document first	A configuration export from the system; privileged access records
A.8.20	Networks security	Close call: an assessor reviews the cited document first	An endpoint configuration export; a firewall rule review; a current network diagram

Control	Title	Why it is listed	Evidence to collect
A.8.3	Information access restriction	Close call: an assessor reviews the cited document first	Privileged access records; access control records (user and role listings); an approved policy
A.8.7	Protection against malware	Close call: an assessor reviews the cited document first	An endpoint configuration export; backup job records; training completion records
A.8.8	Management of technical vulnerabilities	Close call: an assessor reviews the cited document first	A vulnerability scan report; patching records; an assessment record
10.2	Nonconformity and corrective action	The documents cited do not show it	An assessment record; an extract from the relevant register; an approved plan
4.4	Information security management system	The documents cited do not show it	A governance record (minutes or a decision record); a documented procedure
5.1	Leadership and commitment	The documents cited do not show it	A governance record (minutes or a decision record); an approved policy
6.1	Actions to address risks and opportunities	The documents cited do not show it	An assessment record; an extract from the relevant register; a risk assessment
6.2	Information security objectives and planning	The documents cited do not show it	A governance record (minutes or a decision record); an approved plan
6.3	Planning of changes	The documents cited do not show it	A signed review record; a governance record (minutes or a decision record); an approved plan
7.4	Communication	The documents cited do not show it	A governance record (minutes or a decision record); a documented procedure
8.2	Information security risk assessment	The documents cited do not show it	A signed review record; an assessment record; a risk assessment
8.3	Information security risk treatment	The documents cited do not show it	A risk assessment; an approved plan; a documented procedure
9.2	Internal audit	The documents cited do not show it	Audit records; a governance record (minutes or a decision record); an approved plan
9.3	Management review	The documents cited do not show it	A signed review record; a governance record (minutes or a decision record); an approved plan
A.5.10	Acceptable use of information and other associated assets	The documents cited do not show it	Access control records (user and role listings); an extract from the relevant register; an approved policy
A.5.12	Classification of information	The documents cited do not show it	An extract from the relevant register; a documented procedure
A.5.13	Labelling of information	The documents cited do not show it	An extract from the relevant register; a documented procedure
A.5.14	Information transfer	The documents cited do not show it	Key management records; a documented procedure
A.5.15	Access control	The documents cited do not show it	A log extract; privileged access records; access control records (user and role listings)
A.5.18	Access rights	The documents cited do not show it	Access control records (user and role listings); a signed review record; a governance record (minutes or a decision record)
A.5.20	Addressing information security within supplier agreements	The documents cited do not show it	Incident records; supplier assurance reports; the relevant contract clauses
A.5.23	Information security for use of cloud services	The documents cited do not show it	The relevant contract clauses; a shared responsibility matrix; a governance record (minutes or a decision record)
A.5.25	Assessment and decision on information security events	The documents cited do not show it	Incident records; an assessment record; an extract from the relevant register
A.5.27	Learning from information security incidents	The documents cited do not show it	Incident records; a signed review record
A.5.28	Collection of evidence	The documents cited do not show it	Incident records; a governance record (minutes or a decision record); a documented procedure

Control	Title	Why it is listed	Evidence to collect
A.5.29	Information security during disruption	The documents cited do not show it	An approved plan
A.5.3	Segregation of duties	The documents cited do not show it	A governance record (minutes or a decision record); a documented procedure
A.5.30	ICT readiness for business continuity	The documents cited do not show it	A configuration export from the system; backup job records; an exercise record
A.5.31	Legal, statutory, regulatory and contractual requirements	The documents cited do not show it	Audit records; an extract from the relevant register; the relevant contract clauses
A.5.32	Intellectual property rights	The documents cited do not show it	Audit records; an extract from the relevant register; a documented procedure
A.5.33	Protection of records	The documents cited do not show it	Access control records (user and role listings)
A.5.34	Privacy and protection of PII	The documents cited do not show it	An extract from the relevant register; a documented procedure
A.5.4	Management responsibilities	The documents cited do not show it	A governance record (minutes or a decision record); a documented procedure
A.5.6	Contact with special interest groups	The documents cited do not show it	A governance record (minutes or a decision record)
A.5.7	Threat intelligence	The documents cited do not show it	A risk assessment
A.5.8	Information security in project management	The documents cited do not show it	A risk assessment
A.5.9	Inventory of information and other associated assets	The documents cited do not show it	An assessment record; an extract from the relevant register; a risk assessment
A.6.1	Screening	The documents cited do not show it	An extract from the relevant register; a governance record (minutes or a decision record); a documented procedure
A.6.2	Terms and conditions of employment	The documents cited do not show it	A governance record (minutes or a decision record)
A.6.4	Disciplinary process	The documents cited do not show it	A governance record (minutes or a decision record); a documented procedure; an approved policy
A.6.5	Responsibilities after termination or change of employment	The documents cited do not show it	Access control records (user and role listings); a signed review record; a governance record (minutes or a decision record)
A.6.7	Remote working	The documents cited do not show it	A configuration export from the system; an endpoint configuration export; access control records (user and role listings)
A.6.8	Information security event reporting	The documents cited do not show it	Incident records
A.7.1	Physical security perimeters	The documents cited do not show it	An extract from the relevant register; a documented procedure
A.7.10	Storage media	The documents cited do not show it	An extract from the relevant register; a documented procedure
A.7.11	Supporting utilities	The documents cited do not show it	A configuration export from the system; backup job records; an approved plan
A.7.12	Cabling security	The documents cited do not show it	A documented procedure
A.7.13	Equipment maintenance	The documents cited do not show it	An authorisation record; an extract from the relevant register; a documented procedure
A.7.14	Secure disposal or re-use of equipment	The documents cited do not show it	An extract from the relevant register; a documented procedure
A.7.2	Physical entry	The documents cited do not show it	A log extract; access control records (user and role listings); a documented procedure
A.7.3	Securing offices, rooms and facilities	The documents cited do not show it	An extract from the relevant register; a documented procedure

Control	Title	Why it is listed	Evidence to collect
A.7.4	Physical security monitoring	The documents cited do not show it	Monitoring records (alerts and their triage); access control records (user and role listings); audit records
A.7.5	Protecting against physical and environmental threats	The documents cited do not show it	A documented procedure
A.7.6	Working in secure areas	The documents cited do not show it	A governance record (minutes or a decision record); a documented procedure
A.7.7	Clear desk and clear screen	The documents cited do not show it	A documented procedure
A.7.8	Equipment siting and protection	The documents cited do not show it	An extract from the relevant register; a risk assessment; a documented procedure
A.7.9	Security of assets off-premises	The documents cited do not show it	An endpoint configuration export; key management records; an extract from the relevant register
A.8.10	Information deletion	The documents cited do not show it	A configuration export from the system; an endpoint configuration export; a documented procedure
A.8.11	Data masking	The documents cited do not show it	A configuration export from the system; access control records (user and role listings); an extract from the relevant register
A.8.14	Redundancy of information processing facilities	The documents cited do not show it	A configuration export from the system; a documented procedure
A.8.17	Clock synchronisation	The documents cited do not show it	A configuration export from the system; a log extract; an approval record
A.8.21	Security of network services	The documents cited do not show it	Monitoring records (alerts and their triage); a current network diagram
A.8.25	Secure development life cycle	The documents cited do not show it	A signed review record; a documented procedure
A.8.26	Application security requirements	The documents cited do not show it	A signed review record; an approval record; a documented procedure
A.8.27	Secure system architecture and engineering principles	The documents cited do not show it	A signed review record; a documented procedure
A.8.28	Secure coding	The documents cited do not show it	A vulnerability scan report; a signed review record; a documented procedure
A.8.29	Security testing in development and acceptance	The documents cited do not show it	A signed review record; a documented procedure
A.8.30	Outsourced development	The documents cited do not show it	Monitoring records (alerts and their triage); a signed review record; the relevant contract clauses
A.8.31	Separation of development, test and production environments	The documents cited do not show it	A signed review record; a documented procedure
A.8.32	Change management	The documents cited do not show it	A signed review record; an approval record; an authorisation record
A.8.33	Test information	The documents cited do not show it	A configuration export from the system; an extract from the relevant register; a documented procedure
A.8.34	Protection of information systems during audit testing	The documents cited do not show it	Audit records; an approved plan
A.8.4	Access to source code	The documents cited do not show it	Access control records (user and role listings); a signed review record; a documented procedure
A.8.5	Secure authentication	The documents cited do not show it	Access control records (user and role listings); a documented procedure
A.8.6	Capacity management	The documents cited do not show it	Monitoring records (alerts and their triage); an approved plan