SOC 2 Readiness Assessment Report

Aligned to the AICPA Trust Services Criteria (Security / Availability / Confidentiality / Processing Integrity / Privacy)

Organisation / system in scope	Southern Mutual Bank (fictional) / Core banking and customer channels
Framework	SOC 2 (Trust Services Criteria) · AICPA · 2017 TSC (rev. 2022)
Report type	SOC 2 readiness assessment — documentary review as at the assessment date (not a SOC 2 Type I or Type II report)
Assessment basis / period	As at 2026-11-09
Controls assessed	61
Evidence-led coverage	2 of 61 reached a verdict from evidence
Evidence reach	40 of 61 controls carry uploaded evidence (0 of those also carry a live signal); 21 carry neither
Report number	CS-SMB-2026-002
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 platform-generated readiness assessment of the evidence supplied against the SOC 2 Trust Services Criteria, reviewed as at the assessment date. It does not test operating effectiveness over a period, and it is NOT a SOC 2 Type I or Type II report, a CPA attestation or an opinion: only a licensed CPA firm can issue those. Trust Services Criteria are referenced by identifier with CyberSentien's own paraphrase of each criterion; no AICPA criteria 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 assertion
2	Independent service auditor's report
3	Description of the system (DC §200)
4	Trust Services Criteria, controls, tests of controls and results
5	Exceptions noted
6	CUECs
7	Subservice organisations
8	Changes during the period
9	Evidence freshness statement
10	AI assurance statement
11	SOC 2 (Trust Services Criteria) 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-2026-002
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 SOC 2: 98% proven (0 wrong in 170 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: 52 not confirmed by the AI review. Each lists its candidates and the reason.

Report format and standard alignment

Obligation pack / sources	SOC 2 (Trust Services Criteria) · AICPA
Version	2017 TSC (rev. 2022)
Report format followed	SOC 2 readiness assessment — documentary review as at the assessment date (not a SOC 2 Type I or Type II report)
Primary source cited	https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2
Source access	account

This report follows CyberSentien's own reporting structure for SOC 2 (Trust Services Criteria). 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 assertion
2. Independent service auditor's report
3. Description of the system (DC §200)
4. Trust Services Criteria, controls, tests of controls and results
5. Exceptions noted
6. CUECs
7. Subservice organisations
8. Changes during the period

Companion artefacts in this framework's report family: SOC 2 readiness report, TSC control matrix, system description, CUEC register, subservice-org register, exceptions register, evidence register, CPA handoff pack.

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	21
implemented (of evidence-led)	gaps / not met	manual assessment required

Against SOC 2 (Trust Services Criteria), 2 of 61 controls were assessed from evidence (continuous signals and the assessor's uploaded evidence), of which 0 are implemented, 2 partially, and 0 are gaps. 21 controls have no automated signal or uploaded evidence and require assessor review. A further 38 are outstanding: 35 candidate evidence — assessor review; 3 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): Common Criteria — logical & physical access (1), Common Criteria — system operations (1).

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 Common Criteria — logical & physical access	1 control are partially evidenced — working practice exists but would not fully withstand assurance challenge.	CC6.3
NEXT	Strengthen Common Criteria — system operations	1 control are partially evidenced — working practice exists but would not fully withstand assurance challenge.	CC7.2

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 24 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	61
Controls with a document cited against them	40
Controls the document matcher put forward from the documents, each read by the AI review	40
Confirmed by the AI review and shown as a credit, with the passage it rests on	2
Refused by the AI review: the documents cited do not show the control	23
Close calls the AI review left for an assessor to decide	15
Controls with no document cited, so nothing for the AI review to read	21
The AI review's tested accuracy for SOC 2	170 of 170 credits right (100%) in an independent test on fictional evidence

1. Management assertion

The service organisation's own written assertion about its system and the suitability of control design and operating effectiveness. Provided and signed by management — it is not an engine output.

Status: **not part of this readiness assessment**. Management writes and signs it for the SOC examination; nothing in this report is management's assertion.

2. Independent service auditor's report

The independent service auditor's opinion. Issued only by a licensed CPA firm following an AICPA AT-C 205 / SSAE 18 examination. CyberSentien does not and cannot issue it; this report is readiness evidence prepared for that examination.

Status: **not part of this readiness assessment**. Only a licensed CPA firm issues it, as its own report after its own examination. The heading is shown so a reader can see where it sits in a SOC report.

3. Description of the system (DC §200)

This section carries the system boundary, the in-scope services and the assessment method as the engine resolved them. A complete DC §200 description is management's own, and additionally covers the infrastructure, software, people, procedures and data, the principal service commitments and system requirements, and the relevant aspects of the control environment.

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

3a. 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 40 controls assessed here, so nothing in this report rests on continuous validation. A further 21 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.

3b. 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.

Reading. Reader coverage for this framework — cited (document, control) pairs read: 76 of 76. Credited with a quoted passage: 1. Shown as candidate evidence for assessor review: 39, of which 0 were credited by the deterministic assessment and appear here for confirmation rather than as gaps.

4. Trust Services Criteria, controls, tests of controls and results

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

Common Criteria — control environment (5)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
CC1.1	Commitment to integrity and ethical values	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.
CC1.2	Board oversight independence	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…` *"Southern Mutual Bank — Internal Use Only · UNCONTROLLED WHEN PRINTED · SYNTHETIC TEST DOCUMENT Page 2 4.1.1 Accountability for each control area shall be assigned to a named executive owner reporting to the Board Risk Committee."* 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.
CC1.3	Structures, reporting lines and authority	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…` *"Purpose and control objectives This governance establishes the requirements, accountabilities and control objectives for security governance committee charter 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
CC1.4	Commitment to 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)	043_personnel_security_screening_onboarding_offboarding_procedure.pdf · `463bd5f5a183…` 128_security_awareness_training_completion_report_q2_2026.pdf · `15697abedbea…` 218_security_awareness_training_completion_report_q3_2025.pdf · `440dd0e6d2e4…` *"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.
CC1.5	Accountability	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.

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

Common Criteria — communication & information (3)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
CC2.1	Relevant quality information	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.
CC2.2	Internal communication	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…` *"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.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
CC2.3	External communication	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.

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

Common Criteria — risk assessment (4)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
CC3.1	Objectives for risk assessment	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** close call (an assessor decides)	052_audit_findings_risk_treatment_register.pdf · `5cc25603c344`… *"Register entries ID Risk / finding Likelihood x impact Risk owner Treatment plan Residual risk / status AUD-001 Internal audit finding — privileged access recertification evidence incomplete Possible x Major = High Mei-Lin Tan Compensating control in place; risk assessment refreshed High — OUTSIDE APPETITE, escalated to Board Risk Committee AUD-002 External audit finding — backup restoration test"* Where this evidence covers one site, system or incident, confirm the same holds across the whole organisation.	Insufficient evidence	Provide evidence to enable an evidence-led result.
CC3.2	Risk identification and analysis	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.
CC3.3	Fraud risk	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`… *"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.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
CC3.4	Changes affecting internal 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	053_security_testing_assurance_procedure.pdf · `62b4dd18699d…` *"Southern Mutual Bank — Internal Use Only · UNCONTROLLED WHEN PRINTED · SYNTHETIC TEST DOCUMENT Page 3 Evidence expected."* 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.*

Common Criteria — monitoring (2)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
CC4.1	Ongoing and separate evaluations	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…` *"4.5.3 An assurance plan shall coordinate internal audit, external assessment and continuous monitoring to avoid gaps and duplication."* 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.
CC4.2	Communicating control deficiencies	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.

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

Common Criteria — control activities (3)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
CC5.1	Control activities to mitigate risk	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…` *"4.2.2 Risks shall be identified, assessed, treated and tracked in the enterprise risk register with accountable owners."* 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
CC5.2	General controls over technology	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…` *"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.
CC5.3	Controls via policies and 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)	001_information_security_policy.pdf · `19b799381535…` 046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` *"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.

*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.*

Common Criteria — logical & physical access (8)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
CC6.1	Logical access security	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.
CC6.2	User registration and authorisation	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
CC6.3	Role-based access and least privilege	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`… *"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)	Role-based access and least privilege — 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.
CC6.4	Physical access restriction	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.
CC6.5	Secure disposal of 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	041_physical_environmental_security_policy.pdf · `d0fa967acaaf`… *"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.
CC6.6	Boundary protection	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
CC6.7	Protection of information in transit	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…` *"Requirements 4.1 Information handling and data protection 4.1.1 Personal information and other sensitive records shall be handled per their classification: collected only for a documented purpose, accessed on a need-to-know basis, encrypted in transit and at rest, and never sent to unapproved services or personal accounts."* 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.
CC6.8	Malicious software prevention	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.

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

Common Criteria — system operations (5)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
CC7.1	Vulnerability and configuration monitoring	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…` 1240_powershell_and_process_creation_auditing_configuration_export_windows_fleet.pdf · `9e603bbcafff…` 1235_wdac_application_control_policy_configuration_export_workstations_and_servers.pdf · `c128df5d52ea…` *"What this export is A configuration export for Windows Fleet: 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.	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
CC7.2	Anomaly monitoring	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…` 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.	Partially implemented (exception)	Anomaly monitoring — touched by the evidence assessed against it (4 cited documents) but not established by it. (evidence route: uploaded evidence) — Remediate and provide evidence for re-validation.
CC7.3	Security event 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…` 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.	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
CC7.4	Incident response	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.
CC7.5	Incident recovery	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** close call (an assessor decides)	011_data_breach_response_procedure.pdf · `4bc5e0e094ad…` 208_incident_post_mortem_q3_2025.pdf · `72971ff13676…` 118_incident_post_mortem_q2_2026.pdf · `ee3caab338c2…` *"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.	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.*

Common Criteria — change management (1)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
CC8.1	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…` *"4.4 Change management and change control 4.4.1 All changes to production systems, applications, configurations and infrastructure shall be raised as change records, risk-assessed, tested and approved by the Change Advisory Board or, for pre-approved standard changes, by the change 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.

*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.*

Common Criteria — risk mitigation (2)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
CC9.1	Business disruption risk mitigation	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)	032_operational_resilience_policy_cps_230.pdf · `4027f4cd46d7…` 013_disaster_recovery_plan.pdf · `43e28b398d1d…` 014_backup_restoration_standard.pdf · `9342ac709c37…` *"4.3.3 Business continuity arrangements shall address workforce, workplace, technology and supplier dependencies."* 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.
CC9.2	Vendor and partner risk	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.

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

Availability (3)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
A1.1	Capacity management	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.
A1.2	Environmental protections and backup	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)	032_operational_resilience_policy_cps_230.pdf · `4027f4cd46d7…` 014_backup_restoration_standard.pdf · `9342ac709c37…` 133_backup_jobs_report_core_banking_temenos_t24_q2_2026.pdf · `07156e0422ea…` *"Southern Mutual Bank — Internal Use Only · UNCONTROLLED WHEN PRINTED · SYNTHETIC TEST DOCUMENT Page 2 Setting Value Status Environmental protections Backup and recovery infrastructure with redundancy; environmental protections at both sites Compliant 4."* 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.
A1.3	Recovery testing	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)	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)* *"Restoration and recovery testing Setting Value Status Restore test Restoration drill passed 12 days ago — data restored to test systems; recovery time objective met Pass Recovery plan procedures Recovery plan procedures tested; disaster recovery exercise report on file Pass Alternate telecommunication services Alternate telecommunication services tested quarterly Pass Backup retention Retention"* 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.*

Confidentiality (2)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
C1.1	Identifying confidential 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)	046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` *"Purpose and control objectives This procedure establishes the requirements, accountabilities and control objectives for records management & data handling 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.
C1.2	Disposal of confidential 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	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.

*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.*

Processing integrity (5)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
PI1.1	Processing information definitions	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…` *"Purpose and control objectives This procedure establishes the requirements, accountabilities and control objectives for records management & data handling 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.

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
PI1.2	Input controls	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.
PI1.3	Processing controls	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…` *"This provides assurance that the control operates effectively over time."* 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.
PI1.4	Output controls	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…` *"Purpose and control objectives This procedure establishes the requirements, accountabilities and control objectives for records management & data handling 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.
PI1.5	Storage integrity	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…` *"Purpose and control objectives This procedure establishes the requirements, accountabilities and control objectives for records management & data handling 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.

*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.*

Privacy (18)

Control	Name / area	Test of control	Evidence (cited · SHA-256)	Result	Finding / remediation
P1.1	Privacy notice	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)	047_personal_information_handling_procedure.pdf · `dc109a6f6de6…` 022_privacy_policy.pdf · `e9579dc88cc5…` *"Requirements 4.1 Collection, use and disclosure"* 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.
P2.1	Choice and consent	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	047_personal_information_handling_procedure.pdf · `dc109a6f6de6…` 022_privacy_policy.pdf · `e9579dc88cc5…` *"Requirements 4.1 Collection, use and disclosure"* 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.
P3.1	Collection consistent with objectives	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.
P3.2	Explicit consent for sensitive data	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.
P4.1	Use limitation	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	047_personal_information_handling_procedure.pdf · `dc109a6f6de6…` 022_privacy_policy.pdf · `e9579dc88cc5…` 038_data_retention_disposal_standard.pdf · `7763782c1a38…` *"4.3.2 Records shall be retained for their retention period and no longer; over-retention of personal information is prohibited and shall be reported as a privacy compliance gap."* 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
P4.2	Retention	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…` 022_privacy_policy.pdf · `e9579dc88cc5…` 038_data_retention_disposal_standard.pdf · `7763782c1a38…` *"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.
P4.3	Disposal of personal 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	046_records_management_data_handling_procedure.pdf · `291c9ae746a6…` 038_data_retention_disposal_standard.pdf · `7763782c1a38…` *"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.
P5.1	Data-subject access	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.
P5.2	Correction of personal information	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
P6.1	Disclosure with consent	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	047_personal_information_handling_procedure.pdf · `dc109a6f6de6…` 022_privacy_policy.pdf · `e9579dc88cc5…` *"4.1.3 Transfers of personal information to third parties or across borders shall be authorised, covered by contract and recorded in the transfer register."* 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.
P6.2	Record of authorised disclosures	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	047_personal_information_handling_procedure.pdf · `dc109a6f6de6…` 022_privacy_policy.pdf · `e9579dc88cc5…` 038_data_retention_disposal_standard.pdf · `7763782c1a38…` *"Southern Mutual Bank — Internal Use Only · UNCONTROLLED WHEN PRINTED · SYNTHETIC TEST DOCUMENT Page 5 4.4.4 Third-party disclosures of personal information shall occur only under an agreement with appropriate protections, and a record of authorised disclosures (recipient, date, purpose, authority) shall be created and retained in the disclosure register."* 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.
P6.3	Record of unauthorised disclosures	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…` 047_personal_information_handling_procedure.pdf · `dc109a6f6de6…` 022_privacy_policy.pdf · `e9579dc88cc5…` *"Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target."* 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
P6.4	Third-party protections	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.
P6.5	Third-party breach notification	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** not shown by the documents cited	011_data_breach_response_procedure.pdf · `4bc5e0e094ad…` 022_privacy_policy.pdf · `e9579dc88cc5…` *"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.
P6.6	Breach notification	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** not shown by the documents cited	011_data_breach_response_procedure.pdf · `4bc5e0e094ad…` 022_privacy_policy.pdf · `e9579dc88cc5…` *"4.3 Notification and reporting 4.3.1 Reportable incidents shall be notified to APRA within the required timeframe and to the OAIC and affected individuals under the Notifiable Data Breaches scheme where applicable."* 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.
P6.7	Accounting of disclosures	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
P7.1	Data quality	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…` 022_privacy_policy.pdf · `e9579dc88cc5…` *"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.
P8.1	Monitoring and enforcement	Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls **AI review:** no evidence found (no document cited)	—	Manual assessment required	Provide evidence to enable an evidence-led result.

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

4a. Detailed control assessment

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

Common Criteria — control environment (5)

CC1.1 · Commitment to integrity and ethical values — Manual assessment required

Requirement. The entity demonstrates a commitment to integrity and ethical values; code of conduct, tone at the top.

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

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

CC1.2 · Board oversight independence — Candidate evidence — assessor review

Requirement. The board of directors demonstrates independence from management and exercises oversight of internal control.

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

Evidence. 029_security_governance_committee_charter.pdf `e59df87042d8…`

CC1.3 · Structures, reporting lines and authority — Candidate evidence — assessor review

Requirement. Management establishes structures, reporting lines and appropriate authorities and responsibilities.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 029_security_governance_committee_charter.pdf `e59df87042d8…`

CC1.4 · Commitment to competence — Candidate evidence — assessor review

Requirement. The entity demonstrates a commitment to attract, develop and retain competent individuals; hiring, training, competence.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 043_personnel_security_screening_onboarding_offboarding_procedure.pdf `463bd5f5a183`…;
128_security_awareness_training_completion_report_q2_2026.pdf `15697abedbea`…;
218_security_awareness_training_completion_report_q3_2025.pdf `440dd0e6d2e4`…

CC1.5 · Accountability — Manual assessment required

Requirement. The entity holds individuals accountable for their internal control responsibilities; performance, accountability.

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

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

Common Criteria — communication & information (3)

CC2.1 · Relevant quality information — Manual assessment required

Requirement. The entity obtains or generates and uses relevant, quality information to support internal control.

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

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

CC2.2 · Internal communication — Candidate evidence — assessor review

Requirement. The entity internally communicates information, including objectives and responsibilities for internal control; security policies communicated.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 001_information_security_policy.pdf `19b799381535`…

CC2.3 · External communication — Manual assessment required

Requirement. The entity communicates with external parties about matters affecting internal control.

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

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

Common Criteria — risk assessment (4)

CC3.1 · Objectives for risk assessment — Insufficient evidence

Requirement. The entity specifies objectives with sufficient clarity to enable identification and assessment of risks.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 052_audit_findings_risk_treatment_register.pdf `5cc25603c344`…

CC3.2 · Risk identification and analysis — Manual assessment required

Requirement. The entity identifies and analyses risks to the achievement of its objectives; risk assessment process.

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

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

CC3.3 · Fraud risk — Insufficient evidence

Requirement. The entity considers the potential for fraud in assessing risks to the achievement of objectives.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 052_audit_findings_risk_treatment_register.pdf `5cc25603c344`…

CC3.4 · Changes affecting internal control — Candidate evidence — assessor review

Requirement. The entity identifies and assesses changes that could significantly affect the system of internal control.

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

Evidence. 053_security_testing_assurance_procedure.pdf `62b4dd18699d`…

Common Criteria — monitoring (2)

CC4.1 · Ongoing and separate evaluations — Candidate evidence — assessor review

Requirement. The entity selects, develops and performs ongoing and separate evaluations of internal control; control monitoring.

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

Evidence. 040_statement_of_applicability.pdf `692b30be1c54`…

CC4.2 · Communicating control deficiencies — Manual assessment required

Requirement. The entity evaluates and communicates internal control deficiencies to those responsible for corrective action.

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

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

Common Criteria — control activities (3)

CC5.1 · Control activities to mitigate risk — Candidate evidence — assessor review

Requirement. The entity selects and develops control activities that contribute to the mitigation of risks.

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

Evidence. 001_information_security_policy.pdf `19b799381535`…

CC5.2 · General controls over technology — Candidate evidence — assessor review

Requirement. The entity selects and develops general control activities over technology to support objectives.

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

Evidence. 001_information_security_policy.pdf `19b799381535`…

CC5.3 · Controls via policies and procedures — Candidate evidence — assessor review

Requirement. The entity deploys control activities through policies that establish expectations and procedures that put them into action.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 001_information_security_policy.pdf `19b799381535`…; 046_records_management_data_handling_procedure.pdf `291c9ae746a6`…

Common Criteria — logical & physical access (8)

CC6.1 · Logical access security — Manual assessment required

Requirement. Logical access security software, infrastructure and architectures implemented to protect information assets; access control, authentication.

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

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

CC6.2 · User registration and authorisation — Manual assessment required

Requirement. Prior to issuing credentials, users are registered and authorised; provisioning and deprovisioning of access.

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

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

CC6.3 · Role-based access and least privilege — Partially implemented (exception)

Requirement. Access to data and systems is based on roles, least privilege and segregation of duties; access modification and removal.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Confirmed. The AI review credited this control from the documents cited.

Evidence. 1229_privileged_access_configuration_export_pam_platform.pdf `31e96f8caef6`…

Finding & recommendation. Role-based access and least privilege — 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.

CC6.4 · Physical access restriction — Manual assessment required

Requirement. The entity restricts physical access to facilities and protected information assets; data centre and media access.

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

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

CC6.5 · Secure disposal of assets — Candidate evidence — assessor review

Requirement. The entity discontinues logical and physical protections over assets only after the ability to read or recover data is removed; secure disposal.

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

Evidence. 041_physical_environmental_security_policy.pdf `d0fa967acaaf`…

CC6.6 · Boundary protection — Manual assessment required

Requirement. The entity implements boundary protection to protect against threats from outside its system boundaries; firewalls, perimeter.

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

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

CC6.7 · Protection of information in transit — Candidate evidence — assessor review

Requirement. The entity restricts the transmission, movement and removal of information and protects it during transit; encryption in transit, DLP.

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

Evidence. 046_records_management_data_handling_procedure.pdf `291c9ae746a6`…

CC6.8 · Malicious software prevention — Manual assessment required

Requirement. The entity detects and prevents the introduction of unauthorised or malicious software; anti-malware, allowlisting.

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

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

Common Criteria — system operations (5)

CC7.1 · Vulnerability and configuration monitoring — Candidate evidence — assessor review

Requirement. The entity uses detection and monitoring to identify configuration changes and new vulnerabilities; vulnerability scanning.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 008_logging_monitoring_policy.pdf `808a97e670d8`…; 1240_powershell_and_process_creation_auditing_configuration_export_windows_fleet.pdf `9e603bbcafff`…; 1235_wdac_application_control_policy_configuration_export_workstations_and_servers.pdf `c128df5d52ea`…

CC7.2 · Anomaly monitoring — Partially implemented (exception)

Requirement. The entity monitors system components for anomalies indicative of malicious acts, errors and disasters; security monitoring, SIEM.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Confirmed. The AI review credited this control from the documents cited.

Evidence. 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`…; 207_soc_monitoring_report_q3_2025.pdf `bace47f7be25`…

Finding & recommendation. Anomaly monitoring — touched by the evidence assessed against it (4 cited documents) but not established by it. (evidence route: uploaded evidence) Remediate and provide evidence for re-validation.

CC7.3 · Security event evaluation — Candidate evidence — assessor review

Requirement. The entity evaluates security events to determine whether they could result in a failure to meet objectives (incidents).

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 008_logging_monitoring_policy.pdf `808a97e670d8`…; 117_soc_monitoring_report_q2_2026.pdf `06ca0cc7ca28`…; 207_soc_monitoring_report_q3_2025.pdf `bace47f7be25`…

CC7.4 · Incident response — Insufficient evidence

Requirement. The entity responds to identified security incidents by executing a defined incident response programme; containment, remediation.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 208_incident_post_mortem_q3_2025.pdf `72971ff13676`…; 118_incident_post_mortem_q2_2026.pdf `ee3caab338c2`…

CC7.5 · Incident recovery — Candidate evidence — assessor review

Requirement. The entity identifies, develops and implements activities to recover from identified security incidents.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 011_data_breach_response_procedure.pdf `4bc5e0e094ad`…; 208_incident_post_mortem_q3_2025.pdf `72971ff13676`…; 118_incident_post_mortem_q2_2026.pdf `ee3caab338c2`…

Common Criteria — change management (1)

CC8.1 · Change management — Candidate evidence — assessor review

Requirement. The entity authorises, designs, develops, tests, approves and implements changes to infrastructure, data and software; change control.

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

Evidence. 053_security_testing_assurance_procedure.pdf `62b4dd18699d`…

Common Criteria — risk mitigation (2)

CC9.1 · Business disruption risk mitigation — Candidate evidence — assessor review

Requirement. The entity identifies, selects and develops risk mitigation activities for business disruptions; business continuity, resilience.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 032_operational_resilience_policy_cps_230.pdf `4027f4cd46d7`…; 013_disaster_recovery_plan.pdf `43e28b398d1d`…; 014_backup_restoration_standard.pdf `9342ac709c37`…

CC9.2 · Vendor and partner risk — Manual assessment required

Requirement. The entity assesses and manages risks associated with vendors and business partners; third-party risk management.

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

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

Availability (3)

A1.1 · Capacity management — Manual assessment required

Requirement. The entity maintains, monitors and evaluates current processing capacity and use of capacity to meet availability objectives.

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

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

A1.2 · Environmental protections and backup — Candidate evidence — assessor review

Requirement. The entity provides environmental protections, backup and recovery infrastructure to meet availability objectives; redundancy, backups.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 032_operational_resilience_policy_cps_230.pdf `4027f4cd46d7`…; 014_backup_restoration_standard.pdf `9342ac709c37`…; 133_backup_jobs_report_core_banking_temenos_t24_q2_2026.pdf `07156e0422ea`…

A1.3 · Recovery testing — Candidate evidence — assessor review

Requirement. The entity tests recovery plan procedures supporting system recovery to meet availability objectives; DR testing.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 032_operational_resilience_policy_cps_230.pdf `4027f4cd46d7`…; 013_disaster_recovery_plan.pdf `43e28b398d1d`…; 014_backup_restoration_standard.pdf `9342ac709c37`…; 133_backup_jobs_report_core_banking_temenos_t24_q2_2026.pdf `07156e0422ea`…

Confidentiality (2)

C1.1 · Identifying confidential information — Candidate evidence — assessor review

Requirement. The entity identifies and maintains confidential information to meet confidentiality objectives; data classification.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 046_records_management_data_handling_procedure.pdf `291c9ae746a6`…

C1.2 · Disposal of confidential information — Candidate evidence — assessor review

Requirement. The entity disposes of confidential information to meet confidentiality objectives; secure disposal, retention.

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

Evidence. 041_physical_environmental_security_policy.pdf `d0fa967acaaf`…

Processing integrity (5)

PI1.1 · Processing information definitions — Candidate evidence — assessor review

Requirement. The entity obtains or generates relevant, quality information about processing objectives and system inputs and outputs.

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

Evidence. 046_records_management_data_handling_procedure.pdf `291c9ae746a6`…

PI1.2 · Input controls — Manual assessment required

Requirement. The entity implements controls over inputs to result in complete and accurate processing; input validation.

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

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

PI1.3 · Processing controls — Candidate evidence — assessor review

Requirement. The entity implements controls over processing to result in complete, accurate and timely processing.

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

Evidence. 046_records_management_data_handling_procedure.pdf `291c9ae746a6`…

PI1.4 · Output controls — Candidate evidence — assessor review

Requirement. The entity implements controls over outputs to meet processing integrity objectives.

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

Evidence. 046_records_management_data_handling_procedure.pdf `291c9ae746a6`…

PI1.5 · Storage integrity — Candidate evidence — assessor review

Requirement. The entity stores inputs, items in processing and outputs completely, accurately and timely to meet processing integrity objectives.

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

Evidence. 046_records_management_data_handling_procedure.pdf `291c9ae746a6`…

Privacy (18)

P1.1 · Privacy notice — Candidate evidence — assessor review

Requirement. The entity provides notice about the collection, use, retention, disclosure and disposal of personal information; privacy notice.

Assessment. Documentary review of uploaded evidence, as at the assessment date — Uploaded evidence assessed against this framework's own controls.
AI review. Close call. The AI review read the documents cited and was not sure enough to credit this control; an assessor decides.

Evidence. 047_personal_information_handling_procedure.pdf `dc109a6f6de6`…; 022_privacy_policy.pdf `e9579dc88cc5`…

P2.1 · Choice and consent — Candidate evidence — assessor review

Requirement. The entity communicates choices available and obtains consent for the collection, use and disclosure of personal information.

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

Evidence. 047_personal_information_handling_procedure.pdf `dc109a6f6de6`…; 022_privacy_policy.pdf `e9579dc88cc5`…

P3.1 · Collection consistent with objectives — Manual assessment required

Requirement. Personal information is collected consistent with the entity's objectives related to privacy.

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

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

P3.2 · Explicit consent for sensitive data — Manual assessment required

Requirement. The entity obtains explicit consent for sensitive personal information where required.

Assessment. No automated signal or uploaded evidence is currently mapped to this control — assessor review required.
AI review. No evidence found. No document in the evidence pack is cited for this control, so there was nothing for the AI review to read.

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

P4.1 · Use limitation — Candidate evidence — assessor review

Requirement. The entity limits the use of personal information to the purposes identified in the privacy notice and for which consent was obtained.

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

Evidence. 047_personal_information_handling_procedure.pdf `dc109a6f6de6…`; 022_privacy_policy.pdf `e9579dc88cc5…`; 038_data_retention_disposal_standard.pdf `7763782c1a38…`

P4.2 · Retention — Candidate evidence — assessor review

Requirement. The entity retains personal information consistent with the entity's objectives related to privacy; retention limits.

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

Evidence. 046_records_management_data_handling_procedure.pdf `291c9ae746a6…`; 022_privacy_policy.pdf `e9579dc88cc5…`; 038_data_retention_disposal_standard.pdf `7763782c1a38…`

P4.3 · Disposal of personal information — Candidate evidence — assessor review

Requirement. The entity securely disposes of personal information to meet privacy objectives.

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

Evidence. 046_records_management_data_handling_procedure.pdf `291c9ae746a6…`; 038_data_retention_disposal_standard.pdf `7763782c1a38…`

P5.1 · Data-subject access — Manual assessment required

Requirement. The entity grants identified data subjects access to their personal information for review and correction.

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

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

P5.2 · Correction of personal information — Manual assessment required

Requirement. The entity corrects, amends or appends personal information based on data-subject requests.

Assessment. No automated signal or uploaded evidence is currently mapped to this control — assessor review required.
AI review. No evidence found. No document in the evidence pack is cited for this control, so there was nothing for the AI review to read.

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

P6.1 · Disclosure with consent — Candidate evidence — assessor review

Requirement. The entity discloses personal information to third parties only for identified purposes and with consent.

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

Evidence. 047_personal_information_handling_procedure.pdf `dc109a6f6de6…`; 022_privacy_policy.pdf `e9579dc88cc5…`

P6.2 · Record of authorised disclosures — Candidate evidence — assessor review

Requirement. The entity creates and retains a record of authorised disclosures of personal information.

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

Evidence. 047_personal_information_handling_procedure.pdf `dc109a6f6de6…`; 022_privacy_policy.pdf `e9579dc88cc5…`; 038_data_retention_disposal_standard.pdf `7763782c1a38…`

P6.3 · Record of unauthorised disclosures — Candidate evidence — assessor review

Requirement. The entity creates and retains a record of detected or reported unauthorised disclosures of personal information.

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

Evidence. 011_data_breach_response_procedure.pdf `4bc5e0e094ad…`; 047_personal_information_handling_procedure.pdf `dc109a6f6de6…`; 022_privacy_policy.pdf `e9579dc88cc5…`

P6.4 · Third-party protections — Manual assessment required

Requirement. The entity discloses personal information to third parties only with appropriate agreements and protections in place.

Assessment. No automated signal or uploaded evidence is currently mapped to this control — assessor review required.
AI review. No evidence found. No document in the evidence pack is cited for this control, so there was nothing for the AI review to read.

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

P6.5 · Third-party breach notification — Candidate evidence — assessor review

Requirement. The entity obtains commitments from third parties to notify it of unauthorised disclosures of personal information.

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

Evidence. 011_data_breach_response_procedure.pdf `4bc5e0e094ad…`; 022_privacy_policy.pdf `e9579dc88cc5…`

P6.6 · Breach notification — Candidate evidence — assessor review

Requirement. The entity provides notification of breaches and incidents affecting personal information to affected parties and regulators.

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

Evidence. 011_data_breach_response_procedure.pdf `4bc5e0e094ad…`; 022_privacy_policy.pdf `e9579dc88cc5…`

P6.7 · Accounting of disclosures — Manual assessment required

Requirement. The entity provides data subjects with an accounting of personal information held and responds to enquiries.

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

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

P7.1 · Data quality — Candidate evidence — assessor review

Requirement. The entity collects and maintains accurate, up-to-date, complete and relevant personal information; data quality.

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

Evidence. 046_records_management_data_handling_procedure.pdf `291c9ae746a6…`; 047_personal_information_handling_procedure.pdf `dc109a6f6de6…`; 022_privacy_policy.pdf `e9579dc88cc5…`

P8.1 · Monitoring and enforcement — Manual assessment required

Requirement. The entity monitors compliance with privacy commitments and addresses privacy-related complaints and disputes.

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

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

4b. 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.

4c. 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 8 Implemented / operating effectively (0%) — 1 Partially implemented (exception), 5 Manual assessment required, 2 Candidate evidence — assessor review
Data Protection	0 of 19 Implemented / operating effectively (0%) — 7 Manual assessment required, 12 Candidate evidence — assessor review
Threat Detection	0 of 7 Implemented / operating effectively (0%) — 1 Partially implemented (exception), 1 Insufficient evidence, 1 Manual assessment required, 4 Candidate evidence — assessor review
Incident Response	0 of 6 Implemented / operating effectively (0%) — 2 Manual assessment required, 4 Candidate evidence — assessor review
Governance & Risk	0 of 18 Implemented / operating effectively (0%) — 2 Insufficient evidence, 5 Manual assessment required, 11 Candidate evidence — assessor review
Asset & Configuration	0 of 1 Implemented / operating effectively (0%) — 1 Candidate evidence — assessor review
Other	0 of 2 Implemented / operating effectively (0%) — 1 Manual assessment required, 1 Candidate evidence — assessor review

4d. 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
Common Criteria — control environment	Verified — % of catalogue	0% of catalogue verified	0/5	3	0	0	2
Common Criteria — communication & information	Verified — % of catalogue	0% of catalogue verified	0/3	1	0	0	2
Common Criteria — risk assessment	Verified — % of catalogue	0% of catalogue verified	0/4	3	0	2	1
Common Criteria — monitoring	Evidence on file — % of catalogue	50% of catalogue have evidence on file · 0 verified	0/2	1	0	0	1
Common Criteria — control activities	Verified — % of catalogue	0% of catalogue verified	0/3	3	0	0	0
Common Criteria — logical & physical access	Evidence on file — % of catalogue	38% of catalogue have evidence on file · 0 verified	0/8	3	0	0	5
Common Criteria — system operations	Verified — % of catalogue	0% of catalogue verified	0/5	5	0	1	0

Pillar	Lead KPI	Value	Verified	Evidence on file	At risk	Evidence gap / no visibility	Unassessed
Common Criteria — change management	Verified — % of catalogue	0% of catalogue verified	0/1	1	0	0	0
Common Criteria — risk mitigation	Verified — % of catalogue	0% of catalogue verified	0/2	1	0	0	1
Availability	Verified — % of catalogue	0% of catalogue verified	0/3	2	0	0	1
Confidentiality	Verified — % of catalogue	0% of catalogue verified	0/2	2	0	0	0
Processing integrity	Verified — % of catalogue	0% of catalogue verified	0/5	4	0	0	1
Privacy	Verified — % of catalogue	0% of catalogue verified	0/18	11	0	0	7

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: 3 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.

4e. 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	CC6.1	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
conditional access	CC6.1	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022
privileged roles	CC6.1, CC6.3	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022
guest accounts	CC6.2, CC6.3	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0
dormant accounts	CC6.3, CC6.5	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022
backup execution	A1.2	APRA CPS 230 (Operational Risk), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022
restore testing	A1.3	APRA CPS 230 (Operational Risk), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022

Evidence signal	This framework	Also evidences (other frameworks)
central logging	CC7.2, CC7.3	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	CC7.1	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022
app patching	CC7.1	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0
vulnerability exposure	CC7.1, CC3.2	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	CC6.7, C1.1	APRA CPS 234 (Information Security), Breach Reporting (OAIC NDB / CPS 234), CIS Controls v8, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST SP 800-53 Rev 5
retention	C1.2	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	C1.1	APRA CPS 234 (Information Security), CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST SP 800-53 Rev 5
auth methods	CC6.1	CIS Controls v8, CyberSentien CISSP-aligned Security Practice Assessment, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0
security defaults	CC6.1	APRA CPS 234 (Information Security), CIS Controls v8, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0
application control	CC6.8, CC8.1, CC9.1	APRA CPS 234 (Information Security), CIS Controls v8, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0
device inventory	CC6.1	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	CC6.8	CIS Controls v8, Australian Early Childhood (ECEC — National Law, privacy & child safety), ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0
email security	CC6.6, CC6.8, CC7.4	APRA CPS 234 (Information Security), Breach Reporting (OAIC NDB / CPS 234), CIS Controls v8, ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022
external collaboration	CC6.6, CC6.7	APRA CPS 234 (Information Security), ISO/IEC 27001:2022, SOC 1 (ISAE 3402 / SSAE 18), SOC 3 (Trust Services Criteria — general-use report)
data sharing	CC6.7, C1.1, CC6.6	APRA CPS 234 (Information Security), ISO/IEC 27001:2022, SOC 3 (Trust Services Criteria — general-use report)
identity groups	CC6.1, CC6.3	APRA CPS 234 (Information Security), CIS Controls v8, ISO/IEC 27001:2022, NIST CSF 2.0, PCI DSS v4.0.1, SOC 1 (ISAE 3402 / SSAE 18)
domain verification	CC6.6	APRA CPS 234 (Information Security), ISM / IRAP SAR, ISO/IEC 27001:2022, SOC 3 (Trust Services Criteria — general-use report)
endpoint protection	CC6.8	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	CC7.2, CC7.3, CC4.1	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)

Evidence signal	This framework	Also evidences (other frameworks)
mfa enforced all users	CC6.1	APRA CPS 234 (Information Security), ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)
mfa enforced privileged	CC6.1	APRA CPS 234 (Information Security), ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)
mfa registration complete	CC6.1	ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)
legacy auth blocked	CC6.1	APRA CPS 234 (Information Security), ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)
global admin count bounded	CC6.3	APRA CPS 234 (Information Security), ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)
privileged access standing minimised	CC6.3	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)
inactive unprivileged disabled	CC6.2	APRA CPS 234 (Information Security), ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)
inactive privileged disabled	CC6.2	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)
device compliance complete	CC6.8	APRA CPS 234 (Information Security), ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)
os update ring within month	CC7.1	ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)
application control enforced	CC6.8	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)
office macros internet blocked	CC6.8	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, SOC 3 (Trust Services Criteria — general-use report)
office macros win32 blocked	CC6.8	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, SOC 3 (Trust Services Criteria — general-use report)
office child processes blocked	CC6.8	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, SOC 3 (Trust Services Criteria — general-use report)
office executable content blocked	CC6.8	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, SOC 3 (Trust Services Criteria — general-use report)
office code injection blocked	CC6.8	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, SOC 3 (Trust Services Criteria — general-use report)
pdf child processes blocked	CC6.8	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, SOC 3 (Trust Services Criteria — general-use report)
m365 backup protection active	A1.2	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)
azure backup on schedule	A1.2	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)
azure backup vault immutable	A1.2	ASD Essential Eight, ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)
edr onboarding complete	CC6.8	APRA CPS 234 (Information Security), ISM / IRAP SAR, ISO/IEC 27001:2022, NIST CSF 2.0, SOC 3 (Trust Services Criteria — general-use report)

5. Exceptions noted

#	Control	Area	Nature of exception	Result	Severity
E-1	CC6.3	Role-based access and least privilege	Role-based access and least privilege — touched by the evidence assessed against it (1 cited document) but not established by it. (evidence route: uploaded evidence)	Partially implemented (exception)	Medium
E-2	CC7.2	Anomaly monitoring	Anomaly monitoring — touched by the evidence assessed against it (4 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.

5a. Remediation plan

Phase	Actions	Start	Target	Milestone
Phase 2 — Complete partially met controls	2	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	CC6.3	Partially met — close the gap in Role-based access and least privilege. Evidence that will close it: access control record, governance record, privileged access record, review record.	Identity and access lead	2027-02-07	Evidence re-validation
P2	E-2	CC7.2	Partially met — close the gap in Anomaly monitoring. Evidence that will close it: monitoring record.	IT security operations lead	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.

5b. Evidence-request and remediation register (fast-track)

2 controls to remediate · 35 for the assessor to confirm (candidate evidence on file) · 21 to request from the client · 3 insufficient evidence — the same assessed controls reported throughout this report, grouped into the assessor's working lists.

Pillar	Action	Control	Label	Result
Common Criteria — control environment	Assessor to confirm	CC1.2	Board oversight independence	Candidate evidence — assessor review
Common Criteria — control environment	Assessor to confirm	CC1.3	Structures, reporting lines and authority	Candidate evidence — assessor review
Common Criteria — control environment	Assessor to confirm	CC1.4	Commitment to competence	Candidate evidence — assessor review
Common Criteria — control environment	Request from client	CC1.1	Commitment to integrity and ethical values	Manual assessment required
Common Criteria — control environment	Request from client	CC1.5	Accountability	Manual assessment required

Pillar	Action	Control	Label	Result
Common Criteria — communication & information	Assessor to confirm	CC2.2	Internal communication	Candidate evidence — assessor review
Common Criteria — communication & information	Request from client	CC2.1	Relevant quality information	Manual assessment required
Common Criteria — communication & information	Request from client	CC2.3	External communication	Manual assessment required
Common Criteria — risk assessment	Assessor to confirm	CC3.4	Changes affecting internal control	Candidate evidence — assessor review
Common Criteria — risk assessment	Request from client	CC3.2	Risk identification and analysis	Manual assessment required
Common Criteria — risk assessment	Re-evidence	CC3.1	Objectives for risk assessment	Insufficient evidence
Common Criteria — risk assessment	Re-evidence	CC3.3	Fraud risk	Insufficient evidence
Common Criteria — monitoring	Assessor to confirm	CC4.1	Ongoing and separate evaluations	Candidate evidence — assessor review
Common Criteria — monitoring	Request from client	CC4.2	Communicating control deficiencies	Manual assessment required
Common Criteria — control activities	Assessor to confirm	CC5.1	Control activities to mitigate risk	Candidate evidence — assessor review
Common Criteria — control activities	Assessor to confirm	CC5.2	General controls over technology	Candidate evidence — assessor review
Common Criteria — control activities	Assessor to confirm	CC5.3	Controls via policies and procedures	Candidate evidence — assessor review
Common Criteria — logical & physical access	Remediate	CC6.3	Role-based access and least privilege	Partially implemented (exception)
Common Criteria — logical & physical access	Assessor to confirm	CC6.5	Secure disposal of assets	Candidate evidence — assessor review
Common Criteria — logical & physical access	Assessor to confirm	CC6.7	Protection of information in transit	Candidate evidence — assessor review
Common Criteria — logical & physical access	Request from client	CC6.1	Logical access security	Manual assessment required
Common Criteria — logical & physical access	Request from client	CC6.2	User registration and authorisation	Manual assessment required
Common Criteria — logical & physical access	Request from client	CC6.4	Physical access restriction	Manual assessment required
Common Criteria — logical & physical access	Request from client	CC6.6	Boundary protection	Manual assessment required

Pillar	Action	Control	Label	Result
Common Criteria — logical & physical access	Request from client	CC6.8	Malicious software prevention	Manual assessment required
Common Criteria — system operations	Remediate	CC7.2	Anomaly monitoring	Partially implemented (exception)
Common Criteria — system operations	Assessor to confirm	CC7.1	Vulnerability and configuration monitoring	Candidate evidence — assessor review
Common Criteria — system operations	Assessor to confirm	CC7.3	Security event evaluation	Candidate evidence — assessor review
Common Criteria — system operations	Assessor to confirm	CC7.5	Incident recovery	Candidate evidence — assessor review
Common Criteria — system operations	Re-evidence	CC7.4	Incident response	Insufficient evidence
Common Criteria — change management	Assessor to confirm	CC8.1	Change management	Candidate evidence — assessor review
Common Criteria — risk mitigation	Assessor to confirm	CC9.1	Business disruption risk mitigation	Candidate evidence — assessor review
Common Criteria — risk mitigation	Request from client	CC9.2	Vendor and partner risk	Manual assessment required
Availability	Assessor to confirm	A1.2	Environmental protections and backup	Candidate evidence — assessor review
Availability	Assessor to confirm	A1.3	Recovery testing	Candidate evidence — assessor review
Availability	Request from client	A1.1	Capacity management	Manual assessment required
Confidentiality	Assessor to confirm	C1.1	Identifying confidential information	Candidate evidence — assessor review
Confidentiality	Assessor to confirm	C1.2	Disposal of confidential information	Candidate evidence — assessor review
Processing integrity	Assessor to confirm	PI1.1	Processing information definitions	Candidate evidence — assessor review
Processing integrity	Assessor to confirm	PI1.3	Processing controls	Candidate evidence — assessor review
Processing integrity	Assessor to confirm	PI1.4	Output controls	Candidate evidence — assessor review

Pillar	Action	Control	Label	Result
Processing integrity	Assessor to confirm	PI1.5	Storage integrity	Candidate evidence — assessor review
Processing integrity	Request from client	PI1.2	Input controls	Manual assessment required
Privacy	Assessor to confirm	P1.1	Privacy notice	Candidate evidence — assessor review
Privacy	Assessor to confirm	P2.1	Choice and consent	Candidate evidence — assessor review
Privacy	Assessor to confirm	P4.1	Use limitation	Candidate evidence — assessor review
Privacy	Assessor to confirm	P4.2	Retention	Candidate evidence — assessor review
Privacy	Assessor to confirm	P4.3	Disposal of personal information	Candidate evidence — assessor review
Privacy	Assessor to confirm	P6.1	Disclosure with consent	Candidate evidence — assessor review
Privacy	Assessor to confirm	P6.2	Record of authorised disclosures	Candidate evidence — assessor review
Privacy	Assessor to confirm	P6.3	Record of unauthorised disclosures	Candidate evidence — assessor review
Privacy	Assessor to confirm	P6.5	Third-party breach notification	Candidate evidence — assessor review
Privacy	Assessor to confirm	P6.6	Breach notification	Candidate evidence — assessor review
Privacy	Assessor to confirm	P7.1	Data quality	Candidate evidence — assessor review
Privacy	Request from client	P3.1	Collection consistent with objectives	Manual assessment required
Privacy	Request from client	P3.2	Explicit consent for sensitive data	Manual assessment required
Privacy	Request from client	P5.1	Data-subject access	Manual assessment required
Privacy	Request from client	P5.2	Correction of personal information	Manual assessment required

Pillar	Action	Control	Label	Result
Privacy	Request from client	P6.4	Third-party protections	Manual assessment required
Privacy	Request from client	P6.7	Accounting of disclosures	Manual assessment required
Privacy	Request from client	P8.1	Monitoring and enforcement	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.

5c. Residual risk register

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

Catalogue group	Controls	Met	Not met	Partial	Not yet shown	Residual rating	Contributing controls
Common Criteria — logical & physical access	8	0	0	1	7	Medium — default, assessor to confirm	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC6.8
Common Criteria — system operations	5	0	0	1	4	Medium — default, assessor to confirm	CC7.1, CC7.2, CC7.3, CC7.4, CC7.5
Common Criteria — control environment	5	0	0	0	5	To be determined — default, assessor to confirm	CC1.1, CC1.2, CC1.3, CC1.4, CC1.5
Common Criteria — communication & information	3	0	0	0	3	To be determined — default, assessor to confirm	CC2.1, CC2.2, CC2.3
Common Criteria — risk assessment	4	0	0	0	4	To be determined — default, assessor to confirm	CC3.1, CC3.2, CC3.3, CC3.4
Common Criteria — monitoring	2	0	0	0	2	To be determined — default, assessor to confirm	CC4.1, CC4.2
Common Criteria — control activities	3	0	0	0	3	To be determined — default, assessor to confirm	CC5.1, CC5.2, CC5.3
Common Criteria — change management	1	0	0	0	1	To be determined — default, assessor to confirm	CC8.1
Common Criteria — risk mitigation	2	0	0	0	2	To be determined — default, assessor to confirm	CC9.1, CC9.2

Catalogue group	Controls	Met	Not met	Partial	Not yet shown	Residual rating	Contributing controls
Availability	3	0	0	0	3	To be determined — default, assessor to confirm	A1.1, A1.2, A1.3
Confidentiality	2	0	0	0	2	To be determined — default, assessor to confirm	C1.1, C1.2
Processing integrity	5	0	0	0	5	To be determined — default, assessor to confirm	PI1.1, PI1.2, PI1.3, PI1.4, PI1.5
Privacy	18	0	0	0	18	To be determined — default, assessor to confirm	P1.1, P2.1, P3.1, P3.2, P4.1, P4.2, P4.3, P5.1

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.

6. CUECs

Complementary user entity controls — the controls a user organisation must operate for the criteria to be met. Agreed with management before issue.

Status: **not produced by this assessment engine** — to be completed and signed before this report is issued externally. The document-control block above records the issuance state.

7. Subservice organisations

Subservice organisations, the carve-out or inclusive method applied, and the complementary subservice organisation controls. Agreed with management before issue.

Status: **not produced by this assessment engine** — to be completed and signed before this report is issued externally. The document-control block above records the issuance state.

8. Changes during the period

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.

8a. Evidence register

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

#	Control	Cited document	Provenance	Integrity (SHA-256)
1	CC1.2	029_security_governance_committee_charter.pdf	Uploaded evidence	`e59df87042d8710787d77651b1ea20bd7fa9e9a2d76f733608670d68b91b4a35`
2	CC1.3	029_security_governance_committee_charter.pdf	Uploaded evidence	`e59df87042d8710787d77651b1ea20bd7fa9e9a2d76f733608670d68b91b4a35`
3	CC1.4	043_personnel_security_screening_onboarding_offboarding_procedure.pdf	Uploaded evidence	`463bd5f5a183a9e9c20ac5cb95bebec1a734242cfc9c55a4aebfce108c4bf3f9`

#	Control	Cited document	Provenance	Integrity (SHA-256)
4	CC1.4	128_security_awareness_training_completion_report_q2_2026.pdf	Uploaded evidence	15697abedbeafaf40d086d43b7e4884d5230525495036 4a5d04d53e01c583fd9
5	CC1.4	218_security_awareness_training_completion_report_q3_2025.pdf	Uploaded evidence	440dd0e6d2e4be35b9fdf5012696ec11f15be90bf4b5d333f1ef42ce7bfb1b52
6	CC2.2	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e980b10188f726e4e250bec6d8a40da3e43
7	CC3.1	052_audit_findings_risk_treatment_register.pdf	Uploaded evidence	5cc25603c344aeeebeaab3ca11ecd9f9a02128575ef1e8e5c8536da2d21cd56f
8	CC3.3	052_audit_findings_risk_treatment_register.pdf	Uploaded evidence	5cc25603c344aeeebeaab3ca11ecd9f9a02128575ef1e8e5c8536da2d21cd56f
9	CC3.4	053_security_testing_assurance_procedure.pdf	Uploaded evidence	62b4dd18699dada10d686903090f2d5fcd8d6c4dabbf592fb97aca9b27d79adb
10	CC4.1	040_statement_of_applicability.pdf	Uploaded evidence	692b30be1c540b91888388ee79e936198d33644ed5c5f6127ecfff01b25fe82b
11	CC5.1	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e980b10188f726e4e250bec6d8a40da3e43
12	CC5.2	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e980b10188f726e4e250bec6d8a40da3e43
13	CC5.3	001_information_security_policy.pdf	Uploaded evidence	19b799381535e5ed6e887320078e2e980b10188f726e4e250bec6d8a40da3e43
14	CC5.3	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37a7c48f4cb50b5c6c2d37211f2791a516
15	CC6.3	1229_privileged_access_configuration_export_pam_platform.pdf	Uploaded evidence	31e96f8caef6f13a37efb43f0dac8dda728b1b138aa255d7cf04615262507441
16	CC6.5	041_physical_environmental_security_policy.pdf	Uploaded evidence	d0fa967acaaf98dc3a04dd93f060ad537a98613b1b03971f2843e12a55df6ce6
17	CC6.7	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37a7c48f4cb50b5c6c2d37211f2791a516
18	CC7.1	008_logging_monitoring_policy.pdf	Uploaded evidence	808a97e670d8c146b60deffd1db23c48631586d78316946224c5e30f191f36ae
19	CC7.1	1240_powershell_and_process_creation_auditing_configuration_export_windows_fleet.pdf	Uploaded evidence	9e603bbcafff9a0bce830d4398701618ff146a6aded42a8f44461a1741d54b91
20	CC7.1	1235_wdac_application_control_policy_configuration_export_workstations_and_servers.pdf	Uploaded evidence	c128df5d52eab8b3bdadc61313429174ff1f5ecca747e5905df69d25b1005505
21	CC7.2	008_logging_monitoring_policy.pdf	Uploaded evidence	808a97e670d8c146b60deffd1db23c48631586d78316946224c5e30f191f36ae
22	CC7.2	1224_application_control_event_log_extract_workstations_q2_2026.pdf	Uploaded evidence	d8c9185aed6732269e88bc04e603af3abff3d2267a3d20c34a147dfd477f65bb
23	CC7.2	117_soc_monitoring_report_q2_2026.pdf	Uploaded evidence	06ca0cc7ca28d8a40cd52910d13b31e8fc50ffa231af7bccbf6bec614bab39e3
24	CC7.2	207_soc_monitoring_report_q3_2025.pdf	Uploaded evidence	bace47f7be25ed0aa0ce34dabebae7a4fc45755ae7421c6261eb1247ca2c9161
25	CC7.3	008_logging_monitoring_policy.pdf	Uploaded evidence	808a97e670d8c146b60deffd1db23c48631586d78316946224c5e30f191f36ae
26	CC7.3	117_soc_monitoring_report_q2_2026.pdf	Uploaded evidence	06ca0cc7ca28d8a40cd52910d13b31e8fc50ffa231af7bccbf6bec614bab39e3
27	CC7.3	207_soc_monitoring_report_q3_2025.pdf	Uploaded evidence	bace47f7be25ed0aa0ce34dabebae7a4fc45755ae7421c6261eb1247ca2c9161
28	CC7.4	208_incident_post_mortem_q3_2025.pdf	Uploaded evidence	72971ff13676a070d519006e11981d4f404f7a93f71ad11bd0b16108e8cc9b51
29	CC7.4	118_incident_post_mortem_q2_2026.pdf	Uploaded evidence	ee3caab338c2fe87bc753c91d76209313be05224d77f63843081421874d3084b
30	CC7.5	011_data_breach_response_procedure.pdf	Uploaded evidence	4bc5e0e094add1c8bd11f714951f91afccb8ae920e28b586ccbfc49b921601ba
31	CC7.5	208_incident_post_mortem_q3_2025.pdf	Uploaded evidence	72971ff13676a070d519006e11981d4f404f7a93f71ad11bd0b16108e8cc9b51
32	CC7.5	118_incident_post_mortem_q2_2026.pdf	Uploaded evidence	ee3caab338c2fe87bc753c91d76209313be05224d77f63843081421874d3084b

#	Control	Cited document	Provenance	Integrity (SHA-256)
33	CC8.1	053_security_testing_assurance_procedure.pdf	Uploaded evidence	`62b4dd18699dada10d686903090f2d5f cd8d6c4dabbf592fb97aca9b27d79adb`
34	CC9.1	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	`4027f4cd46d73e3ce32e965c8a49a215 e5e432bf08703655d804c28af27dc3b2`
35	CC9.1	013_disaster_recovery_plan.pdf	Uploaded evidence	`43e28b398d1d5644d3719a74fee67c20 af34499386b572d0f34c6bf01675ad6e`
36	CC9.1	014_backup_restoration_standard.pdf	Uploaded evidence	`9342ac709c3737c18af8f9c2eaa8f558 e448604bc0944a018c5f682982da69b9`
37	A1.2	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	`4027f4cd46d73e3ce32e965c8a49a215 e5e432bf08703655d804c28af27dc3b2`
38	A1.2	014_backup_restoration_standard.pdf	Uploaded evidence	`9342ac709c3737c18af8f9c2eaa8f558 e448604bc0944a018c5f682982da69b9`
39	A1.2	133_backup_jobs_report_core_banking_temenos_t24_q2_2026.pdf	Uploaded evidence	`07156e0422eaf1531bcce7f51b3aff44 4265a824cdf9af1a2572007ea2434226`
40	A1.3	032_operational_resilience_policy_cps_230.pdf	Uploaded evidence	`4027f4cd46d73e3ce32e965c8a49a215 e5e432bf08703655d804c28af27dc3b2`
41	A1.3	013_disaster_recovery_plan.pdf	Uploaded evidence	`43e28b398d1d5644d3719a74fee67c20 af34499386b572d0f34c6bf01675ad6e`
42	A1.3	014_backup_restoration_standard.pdf	Uploaded evidence	`9342ac709c3737c18af8f9c2eaa8f558 e448604bc0944a018c5f682982da69b9`
43	A1.3	133_backup_jobs_report_core_banking_temenos_t24_q2_2026.pdf	Uploaded evidence	`07156e0422eaf1531bcce7f51b3aff44 4265a824cdf9af1a2572007ea2434226`
44	C1.1	046_records_management_data_handling_procedure.pdf	Uploaded evidence	`291c9ae746a67e3d6f0e7e28a53abe37 a7c48f4cb50b5c6c2d37211f2791a516`
45	C1.2	041_physical_environmental_security_policy.pdf	Uploaded evidence	`d0fa967acaaf98dc3a04dd93f060ad53 7a98613b1b03971f2843e12a55df6ce6`
46	PI1.1	046_records_management_data_handling_procedure.pdf	Uploaded evidence	`291c9ae746a67e3d6f0e7e28a53abe37 a7c48f4cb50b5c6c2d37211f2791a516`
47	PI1.3	046_records_management_data_handling_procedure.pdf	Uploaded evidence	`291c9ae746a67e3d6f0e7e28a53abe37 a7c48f4cb50b5c6c2d37211f2791a516`
48	PI1.4	046_records_management_data_handling_procedure.pdf	Uploaded evidence	`291c9ae746a67e3d6f0e7e28a53abe37 a7c48f4cb50b5c6c2d37211f2791a516`
49	PI1.5	046_records_management_data_handling_procedure.pdf	Uploaded evidence	`291c9ae746a67e3d6f0e7e28a53abe37 a7c48f4cb50b5c6c2d37211f2791a516`
50	P1.1	047_personal_information_handling_procedure.pdf	Uploaded evidence	`dc109a6f6de6c8620153aec52f4c947b 7d944d2eb0998e85f898eb9f086f3ca3`
51	P1.1	022_privacy_policy.pdf	Uploaded evidence	`e9579dc88cc528afc98aa8e1d6f67d6e 6539bbd161118cbab80be44c4ce0a362`
52	P2.1	047_personal_information_handling_procedure.pdf	Uploaded evidence	`dc109a6f6de6c8620153aec52f4c947b 7d944d2eb0998e85f898eb9f086f3ca3`
53	P2.1	022_privacy_policy.pdf	Uploaded evidence	`e9579dc88cc528afc98aa8e1d6f67d6e 6539bbd161118cbab80be44c4ce0a362`
54	P4.1	047_personal_information_handling_procedure.pdf	Uploaded evidence	`dc109a6f6de6c8620153aec52f4c947b 7d944d2eb0998e85f898eb9f086f3ca3`
55	P4.1	022_privacy_policy.pdf	Uploaded evidence	`e9579dc88cc528afc98aa8e1d6f67d6e 6539bbd161118cbab80be44c4ce0a362`
56	P4.1	038_data_retention_disposal_standard.pdf	Uploaded evidence	`7763782c1a385bad780515fde9aade2c 7a5484acb2a6ff8b12c85a4e0742d3c1`
57	P4.2	046_records_management_data_handling_procedure.pdf	Uploaded evidence	`291c9ae746a67e3d6f0e7e28a53abe37 a7c48f4cb50b5c6c2d37211f2791a516`
58	P4.2	022_privacy_policy.pdf	Uploaded evidence	`e9579dc88cc528afc98aa8e1d6f67d6e 6539bbd161118cbab80be44c4ce0a362`
59	P4.2	038_data_retention_disposal_standard.pdf	Uploaded evidence	`7763782c1a385bad780515fde9aade2c 7a5484acb2a6ff8b12c85a4e0742d3c1`
60	P4.3	046_records_management_data_handling_procedure.pdf	Uploaded evidence	`291c9ae746a67e3d6f0e7e28a53abe37 a7c48f4cb50b5c6c2d37211f2791a516`
61	P4.3	038_data_retention_disposal_standard.pdf	Uploaded evidence	`7763782c1a385bad780515fde9aade2c 7a5484acb2a6ff8b12c85a4e0742d3c1`

#	Control	Cited document	Provenance	Integrity (SHA-256)
62	P6.1	047_personal_information_handling_procedure.pdf	Uploaded evidence	dc109a6f6de6c8620153aec52f4c947b7d944d2eb0998e85f898eb9f086f3ca3
63	P6.1	022_privacy_policy.pdf	Uploaded evidence	e9579dc88cc528afc98aa8e1d6f67d6e6539bbd161118cbab80be44c4ce0a362
64	P6.2	047_personal_information_handling_procedure.pdf	Uploaded evidence	dc109a6f6de6c8620153aec52f4c947b7d944d2eb0998e85f898eb9f086f3ca3
65	P6.2	022_privacy_policy.pdf	Uploaded evidence	e9579dc88cc528afc98aa8e1d6f67d6e6539bbd161118cbab80be44c4ce0a362
66	P6.2	038_data_retention_disposal_standard.pdf	Uploaded evidence	7763782c1a385bad780515fde9aade2c7a5484acb2a6ff8b12c85a4e0742d3c1
67	P6.3	011_data_breach_response_procedure.pdf	Uploaded evidence	4bc5e0e094add1c8bd11f714951f91afccb8ae920e28b586ccbfc49b921601ba
68	P6.3	047_personal_information_handling_procedure.pdf	Uploaded evidence	dc109a6f6de6c8620153aec52f4c947b7d944d2eb0998e85f898eb9f086f3ca3
69	P6.3	022_privacy_policy.pdf	Uploaded evidence	e9579dc88cc528afc98aa8e1d6f67d6e6539bbd161118cbab80be44c4ce0a362
70	P6.5	011_data_breach_response_procedure.pdf	Uploaded evidence	4bc5e0e094add1c8bd11f714951f91afccb8ae920e28b586ccbfc49b921601ba
71	P6.5	022_privacy_policy.pdf	Uploaded evidence	e9579dc88cc528afc98aa8e1d6f67d6e6539bbd161118cbab80be44c4ce0a362
72	P6.6	011_data_breach_response_procedure.pdf	Uploaded evidence	4bc5e0e094add1c8bd11f714951f91afccb8ae920e28b586ccbfc49b921601ba
73	P6.6	022_privacy_policy.pdf	Uploaded evidence	e9579dc88cc528afc98aa8e1d6f67d6e6539bbd161118cbab80be44c4ce0a362
74	P7.1	046_records_management_data_handling_procedure.pdf	Uploaded evidence	291c9ae746a67e3d6f0e7e28a53abe37a7c48f4cb50b5c6c2d37211f2791a516
75	P7.1	047_personal_information_handling_procedure.pdf	Uploaded evidence	dc109a6f6de6c8620153aec52f4c947b7d944d2eb0998e85f898eb9f086f3ca3
76	P7.1	022_privacy_policy.pdf	Uploaded evidence	e9579dc88cc528afc98aa8e1d6f67d6e6539bbd161118cbab80be44c4ce0a362

How the counts relate. This register has one row per control–document citation: 76 citations of 27 distinct documents across 40 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.

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 61 assessed controls with its result, the 27 cited evidence documents by name and the 27 evidence SHA-256 hashes recorded for them.

Distinct evidence artefacts	27
Controls with cited evidence	40
Artefacts carrying a SHA-256 hash	27 of 27
Manifest hash (SHA-256)	bbd2900dce3dde937b02ff39bff07a1e286ed5f71b539beaa3bdf1337280d05f

8c. Quality gate and issuance readiness

Gate check	Status	Detail
Control catalogue assessed	PASS	61 controls assessed
Evidence-led coverage present	PASS	2 of 61 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.

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 27 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 SOC 2 that test result is: 98% proven (0 wrong in 170 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. SOC 2 (Trust Services Criteria) readiness conclusion

Of 61 controls, 2 were assessed from evidence (0 implemented, 0% of those assessed). Outstanding: 2 partially implemented; 21 requiring assessor review — no signal or uploaded evidence; 35 candidate evidence — assessor review; 3 insufficient evidence. This is a platform-generated readiness assessment of the evidence supplied against the SOC 2 Trust Services Criteria, reviewed as at the assessment date. It does not test operating effectiveness over a period, and it is NOT a SOC 2 Type I or Type II report, a CPA attestation or an opinion: only a licensed CPA firm can issue those. Trust Services Criteria are referenced by identifier with CyberSentien's own paraphrase of each criterion; no AICPA criteria 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 · 26 Medium · 35 Low — 61 open controls in all.

Control	Risk	Why rated	Action	Suggested owner (role)	Target date
A1.1	**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
CC1.1	**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
CC1.5	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Identity and access lead	2027-01-08
CC2.1	**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
CC2.3	**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
CC3.1	**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
CC3.2	**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
CC3.3	**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
CC4.2	**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
CC6.1	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Identity and access lead	2027-01-08
CC6.2	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Identity and access lead	2027-01-08
CC6.3	**Medium**	Evidence supports the control only in part	Partially met — close the gap in Role-based access and least privilege. Evidence that will close it: access control record, governance record, privileged access record, review record.	Identity and access lead	2027-01-08
CC6.4	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Identity and access lead	2027-01-08
CC6.6	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Identity and access lead	2027-01-08
CC6.8	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Identity and access lead	2027-01-08
CC7.2	**Medium**	Evidence supports the control only in part	Partially met — close the gap in Anomaly monitoring. Evidence that will close it: monitoring record.	IT security operations lead	2027-01-08
CC7.4	**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
CC9.2	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Third-party risk owner	2027-01-08
P3.1	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Privacy officer	2027-01-08
P3.2	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Privacy officer	2027-01-08
P5.1	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Privacy officer	2027-01-08

Control	Risk	Why rated	Action	Suggested owner (role)	Target date
P5.2	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Privacy officer	2027-01-08
P6.4	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Privacy officer	2027-01-08
P6.7	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Privacy officer	2027-01-08
P8.1	**Medium**	No supporting evidence on file yet	Supply evidence that the control operates: the governing document and operating records	Privacy officer	2027-01-08
PI1.2	**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
A1.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Incident and continuity lead	2027-02-07
A1.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Incident and continuity lead	2027-02-07
C1.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
C1.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
CC1.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
CC1.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
CC1.4	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
CC2.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
CC3.4	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
CC4.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	IT security operations lead	2027-02-07
CC5.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
CC5.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
CC5.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
CC6.5	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Identity and access lead	2027-02-07
CC6.7	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Identity and access lead	2027-02-07

Control	Risk	Why rated	Action	Suggested owner (role)	Target date
CC7.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	IT security operations lead	2027-02-07
CC7.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
CC7.5	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Incident and continuity lead	2027-02-07
CC8.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Engineering lead	2027-02-07
CC9.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
P1.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Privacy officer	2027-02-07
P2.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Privacy officer	2027-02-07
P4.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Privacy officer	2027-02-07
P4.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Privacy officer	2027-02-07
P4.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Privacy officer	2027-02-07
P6.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Privacy officer	2027-02-07
P6.2	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Privacy officer	2027-02-07
P6.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Privacy officer	2027-02-07
P6.5	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Privacy officer	2027-02-07
P6.6	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Privacy officer	2027-02-07
P7.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Privacy officer	2027-02-07
PI1.1	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
PI1.3	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
PI1.4	**Low**	Candidate evidence on file, awaiting assessor confirmation	Assessor to confirm the candidate evidence against the requirement	Information security manager	2027-02-07
PI1.5	**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).*

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
A1.2	Environmental protections and backup	Close call: an assessor reviews the cited document first	A configuration export from the system; backup job records; a governance record (minutes or a decision record)
A1.3	Recovery testing	Close call: an assessor reviews the cited document first	Backup job records; a governance record (minutes or a decision record); an approved plan
C1.1	Identifying confidential information	Close call: an assessor reviews the cited document first	An extract from the relevant register; a governance record (minutes or a decision record); a documented procedure
CC1.3	Structures, reporting lines and authority	Close call: an assessor reviews the cited document first	A governance record (minutes or a decision record)
CC1.4	Commitment to competence	Close call: an assessor reviews the cited document first	Training completion records; a signed review record; a documented procedure
CC2.2	Internal communication	Close call: an assessor reviews the cited document first	A signed review record; a governance record (minutes or a decision record); a documented procedure
CC3.1	Objectives for risk assessment	Close call: an assessor reviews the cited document first	An assessment record; a risk assessment; a governance record (minutes or a decision record)
CC3.3	Fraud risk	Close call: an assessor reviews the cited document first	A risk assessment; a governance record (minutes or a decision record)
CC5.3	Controls via policies and procedures	Close call: an assessor reviews the cited document first	A documented procedure
CC7.1	Vulnerability and configuration monitoring	Close call: an assessor reviews the cited document first	A configuration export from the system; a vulnerability scan report; monitoring records (alerts and their triage)
CC7.3	Security event evaluation	Close call: an assessor reviews the cited document first	Monitoring records (alerts and their triage); incident records; an assessment record
CC7.4	Incident response	Close call: an assessor reviews the cited document first	Incident records
CC7.5	Incident recovery	Close call: an assessor reviews the cited document first	Backup job records; incident records; a signed review record
CC9.1	Business disruption risk mitigation	Close call: an assessor reviews the cited document first	An exercise record; a signed review record; a risk assessment
P1.1	Privacy notice	Close call: an assessor reviews the cited document first	An extract from the relevant register; a governance record (minutes or a decision record); a documented procedure
C1.2	Disposal of confidential information	The documents cited do not show it	An extract from the relevant register; a governance record (minutes or a decision record); a documented procedure
CC1.2	Board oversight independence	The documents cited do not show it	A signed review record; an approval record; a governance record (minutes or a decision record)
CC3.4	Changes affecting internal control	The documents cited do not show it	A signed review record; a governance record (minutes or a decision record)
CC4.1	Ongoing and separate evaluations	The documents cited do not show it	Monitoring records (alerts and their triage); a signed review record; an assessment record
CC5.1	Control activities to mitigate risk	The documents cited do not show it	A signed review record; a risk assessment; a documented procedure
CC5.2	General controls over technology	The documents cited do not show it	A signed review record; a governance record (minutes or a decision record); a documented procedure
CC6.5	Secure disposal of assets	The documents cited do not show it	A log extract; an extract from the relevant register; a documented procedure

Control	Title	Why it is listed	Evidence to collect
CC6.7	Protection of information in transit	The documents cited do not show it	A configuration export from the system; key management records; a current network diagram
CC8.1	Change management	The documents cited do not show it	A signed review record; an approval record; an authorisation record
P2.1	Choice and consent	The documents cited do not show it	An approval record; an extract from the relevant register; a governance record (minutes or a decision record)
P4.1	Use limitation	The documents cited do not show it	An approval record; an extract from the relevant register; a documented procedure
P4.2	Retention	The documents cited do not show it	An extract from the relevant register; a governance record (minutes or a decision record); a documented procedure
P4.3	Disposal of personal information	The documents cited do not show it	An extract from the relevant register; a governance record (minutes or a decision record); a documented procedure
P6.1	Disclosure with consent	The documents cited do not show it	An approval record; an extract from the relevant register; a governance record (minutes or a decision record)
P6.2	Record of authorised disclosures	The documents cited do not show it	An authorisation record; an extract from the relevant register; a governance record (minutes or a decision record)
P6.3	Record of unauthorised disclosures	The documents cited do not show it	An extract from the relevant register; a governance record (minutes or a decision record); a documented procedure
P6.5	Third-party breach notification	The documents cited do not show it	Incident records; an extract from the relevant register; a governance record (minutes or a decision record)
P6.6	Breach notification	The documents cited do not show it	Incident records; an extract from the relevant register; a governance record (minutes or a decision record)
P7.1	Data quality	The documents cited do not show it	An assessment record; an extract from the relevant register; a documented procedure
PI1.1	Processing information definitions	The documents cited do not show it	A governance record (minutes or a decision record); a documented procedure
PI1.3	Processing controls	The documents cited do not show it	A documented procedure
PI1.4	Output controls	The documents cited do not show it	A vulnerability scan report; monitoring records (alerts and their triage); a governance record (minutes or a decision record)
PI1.5	Storage integrity	The documents cited do not show it	A vulnerability scan report; monitoring records (alerts and their triage); a governance record (minutes or a decision record)