Southern Mutual Bank

51 824 753 556

Logging & Monitoring Policy

Policy · synthetic assessor-grade test document

Generated 09 November 2026 · CyberSentien test harness · personalised to Southern Mutual Bank

Document ID	SOU-POL-0008
Version	3.3
Owner	Nadia Petrova (Privacy Counsel)
Approved by	CISO
Classification	Internal Use Only
Status	Approved — In force
Effective date	14 Mar 2026
Next review	14 Mar 2027

1. Purpose and control objectives

This policy establishes the requirements, accountabilities and control objectives for logging & monitoring policy across Southern Mutual Bank (“the Bank”). It forms part of the Bank's Information Security Management System and supports its obligations under ASD ISM, Essential Eight, ISO/IEC 27001:2022, SOC 2 (TSC), APRA CPS 234. It applies to Core banking platform and supporting services.

Control objectives:

• Ensure security-relevant events are captured, protected and retained to support detection and investigation.

• Provide timely detection of, and response to, anomalous and malicious activity.

2. 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.

In scope	Out of scope / exclusions
Production, management and DR environments; Core banking platform; identity, endpoint, network and data services.	Personal devices outside the BYOD programme; non-production sandboxes without Bank data (covered by separate standard).

3. Regulatory and standards context

The requirements herein are designed to satisfy, and are crosswalked to, the following frameworks applicable to a regulated Australian banking entity: ASD ISM, Essential Eight, ISO/IEC 27001:2022, SOC 2 (TSC), APRA CPS 234. Where an obligation is more stringent in one framework, the most stringent requirement applies.

4. Requirements

4.1 Log collection and coverage

4.1.1 Security-relevant events shall be centrally collected, time-synchronised (NTP) and retained for at least 12 months (and longer where regulation requires).

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. 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. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. approved tickets + sign-off records; SIEM / log extract.

Test method. log + exception review. *Frequency.* Monthly. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.1.2 Logging coverage shall be defined per system in a logging matrix and validated against the logging standard at onboarding and annually.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. sampled records + interview notes; scan or test report.

Test method. log + exception review. *Frequency.* Quarterly. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.1.3 Privileged, administrative and authentication events shall always be logged, including success and failure.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. SIEM / log extract; configuration export + change record.

Test method. configuration review + sampling. *Frequency.* Quarterly. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.1.4 Cloud control-plane, identity-provider and endpoint telemetry shall be ingested into the central SIEM.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. 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. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. configuration review + sampling. *Frequency.* Monthly. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2 Detection and alerting

4.2.1 Detection use-cases shall be mapped to relevant threats (e.g. MITRE ATT&CK;) and reviewed at least semi-annually.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. sampled records + interview notes; scan or test report.

Test method. re-performance / observation. *Frequency.* Semi-annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2.2 Alerts shall be triaged within defined response times by severity and escalated per the incident-response process.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. SIEM / log extract; configuration export + change record.

Test method. configuration review + sampling. *Frequency.* Quarterly. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2.3 Alert tuning shall be evidenced to manage false-positive rates without suppressing genuine detections.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. 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. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. log + exception review. *Frequency.* Annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.3 Log integrity and retention

4.3.1 Logs shall be protected against tampering and unauthorised deletion (write-once or access-controlled storage).

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. SIEM / log extract; configuration export + change record.

Test method. log + exception review. *Frequency.* Annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.3.2 Access to the SIEM and log stores shall be least-privilege and itself logged.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. 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. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. automated telemetry review. *Frequency.* Quarterly. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.3.3 Retention and disposal of logs shall follow the records-retention schedule.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is implemented through the IGA/PAM platform with automated workflow and logging.

Evidence expected. configuration export + change record; approved tickets + sign-off records.

Test method. re-performance / observation. *Frequency.* Semi-annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4 Detection engineering and threat coverage

4.4.1 Detections shall be developed, version-controlled and mapped to MITRE ATT&CK; techniques relevant to the threat model.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. 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. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. automated telemetry review. *Frequency.* Quarterly. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4.2 Detection coverage gaps shall be tracked and prioritised; new detections shall be validated before production.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is implemented through the IGA/PAM platform with automated workflow and logging.

Evidence expected. configuration export + change record; approved tickets + sign-off records.

Test method. log + exception review. *Frequency.* Monthly. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4.3 Threat intelligence shall be ingested and operationalised into detections and blocklists.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. tooling dashboard / telemetry extract; sampled records + interview notes.

Test method. re-performance / observation. *Frequency.* Monthly. *Control owner.* Privacy Counsel. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.4.4 Detection efficacy shall be measured (true/false-positive rates) and tuned on a defined cadence.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. 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. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. approved tickets + sign-off records; SIEM / log extract.

Test method. re-performance / observation. *Frequency.* Semi-annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5 Security operations and response readiness

4.5.1 A 24x7 monitoring capability shall triage alerts within severity-based response times with documented shift handover.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is implemented through the IGA/PAM platform with automated workflow and logging.

Evidence expected. configuration export + change record; approved tickets + sign-off records.

Test method. automated telemetry review. *Frequency.* Annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5.2 Runbooks shall exist for high-frequency alert types and be kept current.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. tooling dashboard / telemetry extract; sampled records + interview notes.

Test method. log + exception review. *Frequency.* Monthly. *Control owner.* Privacy Counsel. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.5.3 Threat hunting shall be performed on a defined cadence and findings fed back into detections.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. 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. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. approved tickets + sign-off records; SIEM / log extract.

Test method. re-performance / observation. *Frequency.* Monthly. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5.4 On-call escalation paths and contacts shall be maintained and tested.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. sampled records + interview notes; scan or test report.

Test method. re-performance / observation. *Frequency.* Monthly. *Control owner.* Privacy Counsel. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.6 Governance, accountability and policy lifecycle

4.6.1 A named executive owner shall be accountable for this control area and shall report its status to the Board Risk Committee at least quarterly.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. tooling dashboard / telemetry extract; sampled records + interview notes.

Test method. log + exception review. *Frequency.* Annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.6.2 This document shall be reviewed at least annually and after any material change to the business, technology, regulatory or threat environment, with version control maintained.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. 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. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. approved tickets + sign-off records; SIEM / log extract.

Test method. log + exception review. *Frequency.* Monthly. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.6.3 Roles and responsibilities shall align to the three-lines-of-defence model, with first-line ownership, second-line oversight and third-line independent assurance.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. sampled records + interview notes; scan or test report.

Test method. re-performance / observation. *Frequency.* Annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.6.4 Material decisions, approvals and deviations shall be minuted and retained as part of the governance record.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. SIEM / log extract; configuration export + change record.

Test method. re-performance / observation. *Frequency.* Annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.7 Risk assessment and treatment

4.7.1 Risks within this control area shall be identified, assessed (likelihood × impact), treated and recorded in the enterprise risk register with an accountable owner.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. 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. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. approved tickets + sign-off records; SIEM / log extract.

Test method. log + exception review. *Frequency.* Annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.7.2 Residual risk exceeding the approved risk appetite shall be escalated with a treatment plan and target date.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. sampled records + interview notes; scan or test report.

Test method. log + exception review. *Frequency.* Monthly. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.7.3 Risk assessments shall be refreshed on a defined cadence and upon significant change.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. SIEM / log extract; configuration export + change record.

Test method. re-performance / observation. *Frequency.* Semi-annual. *Control owner.* Privacy Counsel. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.7.4 Key risk indicators (KRIs) shall be defined and monitored against thresholds, with breaches escalated.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. 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. The control is implemented through the IGA/PAM platform with automated workflow and logging.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. re-performance / observation. *Frequency.* Quarterly. *Control owner.* Privacy Counsel. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.8 Monitoring, measurement and reporting

4.8.1 Control performance shall be monitored continuously through automated telemetry into the central assurance platform.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is monitored in the SIEM with detections mapped to the relevant threats.

Evidence expected. sampled records + interview notes; scan or test report.

Test method. re-performance / observation. *Frequency.* Annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.8.2 The metrics and targets in this document shall be reported monthly to the control owner and quarterly to the Executive Risk Committee.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. SIEM / log extract; configuration export + change record.

Test method. configuration review + sampling. *Frequency.* Monthly. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.8.3 Control failures and exceptions shall be logged, triaged by severity and remediated within risk-based timeframes.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. 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. The control is implemented through the IGA/PAM platform with automated workflow and logging.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. re-performance / observation. *Frequency.* Semi-annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.8.4 Independent assurance (internal audit / external assessment) shall periodically test design and operating effectiveness; findings shall be tracked to closure.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. configuration export + change record; approved tickets + sign-off records.

Test method. re-performance / observation. *Frequency.* Annual. *Control owner.* Privacy Counsel. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.9 Records, retention and evidence

4.9.1 Evidence demonstrating the operation of these controls shall be generated, retained and protected per the records-retention schedule.

Control objective / rationale. This provides assurance that the control operates effectively over time.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

Evidence expected. SIEM / log extract; configuration export + change record.

Test method. log + exception review. *Frequency.* Semi-annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.9.2 Evidence shall be sufficient for an independent assessor to conclude on operating effectiveness without reliance on undocumented knowledge.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. 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. The control is implemented through the IGA/PAM platform with automated workflow and logging.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. automated telemetry review. *Frequency.* Annual. *Control owner.* Privacy Counsel. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.9.3 Access to control evidence shall be least-privilege and itself logged; integrity shall be protected against tampering.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. configuration export + change record; approved tickets + sign-off records.

Test method. re-performance / observation. *Frequency.* Quarterly. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.9.4 On decommissioning, records shall be retained or disposed of per the retention schedule and legal hold requirements.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. tooling dashboard / telemetry extract; sampled records + interview notes.

Test method. log + exception review. *Frequency.* Quarterly. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.10 Continuous improvement

4.10.1 Lessons from incidents, audits, assessments and exercises shall be fed back into this control area and the document updated accordingly.

Control objective / rationale. This enforces least privilege, accountability and limits the blast radius of compromise.

Implementation. 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. The control is implemented through the IGA/PAM platform with automated workflow and logging.

Evidence expected. scan or test report; tooling dashboard / telemetry extract.

Test method. log + exception review. *Frequency.* Semi-annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.10.2 Control maturity shall be assessed against a defined target state, with a roadmap to close gaps.

Control objective / rationale. This reduces the likelihood and impact of unauthorised access or control failure.

Implementation. The control owner maintains a documented procedure and the supporting tooling configuration, reviewed on the stated cadence; deviations are routed through the exceptions process with compensating controls. The control is configured per the hardening standard with drift monitoring and alerting.

Evidence expected. configuration export + change record; approved tickets + sign-off records.

Test method. log + exception review. *Frequency.* Semi-annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

4.10.3 Automation and tooling shall be progressively adopted to reduce manual effort and error.

Control objective / rationale. This supports timely detection, response and recovery and meets regulatory obligations.

Implementation. Implementation is automated and enforced through platform policy where feasible, with documented manual compensating steps where automation is not yet available. The control is enforced at the identity provider and gateway with conditional access.

Evidence expected. tooling dashboard / telemetry extract; sampled records + interview notes.

Test method. configuration review + sampling. *Frequency.* Annual. *Control owner.* Privacy Counsel. *Status.* Implemented (self-declared by the document author; not independently verified).

5. Roles and responsibilities (RACI)

Role	R	A	C	I	Responsibility
Privacy Counsel	✓	✓			Owns this document; ensures it is current, resourced and effective.
System / Asset owners	✓		✓		Implement and operate the controls in their scope.

Role	R	A	C	I	Responsibility
Security Operations	✓		✓	✓	Monitors compliance; investigates and responds to exceptions.
Risk & Compliance (2nd line)			✓	✓	Provides oversight, challenge and reporting.
Internal Audit (3rd line)				✓	Independent assurance over design and operating effectiveness.
All staff & contractors	✓			✓	Comply with the requirements; report suspected breaches.

6. Procedures and implementation

6.1 Onboard a system: complete the logging matrix, configure forwarders, validate events reach the SIEM.

6.2 SOC analysts triage alerts on a 24x7 roster with documented handover.

6.3 Threat-hunting is performed on a defined cadence and findings fed back into detections.

7. Monitoring, metrics and KPIs

Metric	Target	Frequency
Critical systems with validated logging	100%	Quarterly
Mean time to triage (high alerts)	≤ 30 min	Monthly
Detection use-cases reviewed	100%	Semi-annual
Log sources reporting (uptime)	≥ 99%	Monthly

8. Compliance, monitoring and enforcement

Compliance is monitored continuously through automated control telemetry, the metrics above and periodic independent assurance. Material non-compliance is recorded in the risk register, escalated to the Executive Risk Committee, and tracked to closure. Wilful or negligent breaches may result in disciplinary action up to termination.

9. Exceptions and waivers

Any deviation requires a documented risk assessment, compensating controls, an expiry date and approval by the accountable risk owner (and the CISO for high-risk deviations). Active exceptions are recorded and reviewed in the Exceptions & Waivers Register.

10. Definitions

Term	Definition
SIEM	Security Information and Event Management — central platform for log analytics and alerting.
Detection use-case	A defined rule/analytic that identifies a specific malicious or anomalous behaviour.
MTTD / MTTR	Mean time to detect / mean time to respond.

11. Related documents

• Information Security Policy

• Security Operations & SIEM Standard

• Incident Response Plan

12. Control framework mapping

Framework	Indicative mapped controls
ASD ISM	Guidelines: Access, System hardening, Monitoring
Essential Eight	ML2 target

Framework	Indicative mapped controls
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23
SOC 2 (TSC)	CC6.1, CC6.2, CC6.3, CC7.2
APRA CPS 234	Information security capability, Control testing, Incident notification

Threat and risk context

This control area addresses the threats and failure modes most relevant to Core banking platform in a regulated Australian banking context — including credential compromise, insider misuse, unmanaged change, third-party failure, data loss and control drift. The requirements in section 4 are calibrated to reduce both the likelihood and the impact of these scenarios, and are tested on the cadence set out in section 7.

- Risk addressed: Ensure security-relevant events are captured, protected and retained to support detection and investigation.
- Risk addressed: Provide timely detection of, and response to, anomalous and malicious activity.

Operating model and continuous assurance

Day-to-day operation follows the three-lines-of-defence model: first-line owners operate the controls and remediate exceptions; second-line risk and compliance provide oversight, challenge and reporting; third-line internal audit provides independent assurance. Control performance is monitored continuously through automated telemetry into the central assurance platform, with monthly control reporting to the control owner and quarterly reporting to the Executive Risk Committee. Deficiencies are recorded in the enterprise risk register and tracked to closure against the targets in section 7.

Training, awareness and competency

Personnel with responsibilities under this document receive role-based training at onboarding and at least annually. General security awareness, including phishing simulation, is delivered to all staff and contractors; completion is tracked and non-completion is escalated to people leaders. Control owners maintain procedures and runbooks sufficient for a competent operator to execute the control consistently, and review them after any material change to the business, technology or threat environment.

Appendix C — Control register (per requirement)

Ref	Control statement	Framework	Test freq.	Status
4.1.1	Security-relevant events shall be centrally collected, time-synchronis…	ASD ISM	Annual	Partially implemented
4.1.2	Logging coverage shall be defined per system in a logging matrix and v…	Essential Eight	Semi-annual	Implemented
4.1.3	Privileged, administrative and authentication events shall always be l…	ISO/IEC 27001:2022	Annual	Partially implemented
4.1.4	Cloud control-plane, identity-provider and endpoint telemetry shall be…	SOC 2 (TSC)	Annual	Partially implemented
4.2.1	Detection use-cases shall be mapped to relevant threats (e.g. MITRE AT…	APRA CPS 234	Monthly	Partially implemented
4.2.2	Alerts shall be triaged within defined response times by severity and …	ASD ISM	Annual	Partially implemented
4.2.3	Alert tuning shall be evidenced to manage false-positive rates without…	Essential Eight	Quarterly	Implemented

Ref	Control statement	Framework	Test freq.	Status
4.3.1	Logs shall be protected against tampering and unauthorised deletion (w…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.3.2	Access to the SIEM and log stores shall be least-privilege and itself …	SOC 2 (TSC)	Annual	Partially implemented
4.3.3	Retention and disposal of logs shall follow the records-retention sche…	APRA CPS 234	Quarterly	Implemented
4.4.1	Detections shall be developed, version-controlled and mapped to MITRE …	ASD ISM	Monthly	Implemented
4.4.2	Detection coverage gaps shall be tracked and prioritised; new detectio…	Essential Eight	Semi-annual	Partially implemented
4.4.3	Threat intelligence shall be ingested and operationalised into detecti…	ISO/IEC 27001:2022	Monthly	Partially implemented
4.4.4	Detection efficacy shall be measured (true/false-positive rates) and t…	SOC 2 (TSC)	Annual	Partially implemented
4.5.1	A 24x7 monitoring capability shall triage alerts within severity-based…	APRA CPS 234	Semi-annual	Implemented
4.5.2	Runbooks shall exist for high-frequency alert types and be kept curren…	ASD ISM	Quarterly	Implemented
4.5.3	Threat hunting shall be performed on a defined cadence and findings fe…	Essential Eight	Quarterly	Implemented
4.5.4	On-call escalation paths and contacts shall be maintained and tested.	ISO/IEC 27001:2022	Semi-annual	Implemented
4.6.1	A named executive owner shall be accountable for this control area and…	SOC 2 (TSC)	Semi-annual	Implemented
4.6.2	This document shall be reviewed at least annually and after any materi…	APRA CPS 234	Monthly	Implemented
4.6.3	Roles and responsibilities shall align to the three-lines-of-defence m…	ASD ISM	Monthly	Implemented
4.6.4	Material decisions, approvals and deviations shall be minuted and reta…	Essential Eight	Semi-annual	Implemented
4.7.1	Risks within this control area shall be identified, assessed (likeliho…	ISO/IEC 27001:2022	Monthly	Implemented
4.7.2	Residual risk exceeding the approved risk appetite shall be escalated …	SOC 2 (TSC)	Annual	Implemented
4.7.3	Risk assessments shall be refreshed on a defined cadence and upon sign…	APRA CPS 234	Semi-annual	Implemented
4.7.4	Key risk indicators (KRIs) shall be defined and monitored against thre…	ASD ISM	Quarterly	Partially implemented
4.8.1	Control performance shall be monitored continuously through automated …	Essential Eight	Semi-annual	Partially implemented
4.8.2	The metrics and targets in this document shall be reported monthly to …	ISO/IEC 27001:2022	Annual	Implemented
4.8.3	Control failures and exceptions shall be logged, triaged by severity a…	SOC 2 (TSC)	Quarterly	Partially implemented
4.8.4	Independent assurance (internal audit / external assessment) shall per…	APRA CPS 234	Quarterly	Implemented

Ref	Control statement	Framework	Test freq.	Status
4.9.1	Evidence demonstrating the operation of these controls shall be genera…	ASD ISM	Monthly	Partially implemented
4.9.2	Evidence shall be sufficient for an independent assessor to conclude o…	Essential Eight	Monthly	Partially implemented
4.9.3	Access to control evidence shall be least-privilege and itself logged;…	ISO/IEC 27001:2022	Annual	Partially implemented
4.9.4	On decommissioning, records shall be retained or disposed of per the r…	SOC 2 (TSC)	Quarterly	Partially implemented
4.10.1	Lessons from incidents, audits, assessments and exercises shall be fed…	APRA CPS 234	Quarterly	Implemented
4.10.2	Control maturity shall be assessed against a defined target state, wit…	ASD ISM	Quarterly	Implemented
4.10.3	Automation and tooling shall be progressively adopted to reduce manual…	Essential Eight	Monthly	Implemented

Appendix A — Control implementation checklist

Control area	Controls	Implementation status
Log collection and coverage	4 control(s)	Implemented
Detection and alerting	3 control(s)	Planned
Log integrity and retention	3 control(s)	Planned
Detection engineering and threat coverage	4 control(s)	Implemented
Security operations and response readiness	4 control(s)	Partially implemented
Governance, accountability and policy lifecycle	4 control(s)	Partially implemented
Risk assessment and treatment	4 control(s)	Implemented
Monitoring, measurement and reporting	4 control(s)	Implemented
Records, retention and evidence	4 control(s)	Implemented
Continuous improvement	3 control(s)	Implemented

Appendix B — Control testing and evidence matrix

Control area	Ctrls	Test method	Evidence	Frequency
Log collection and coverage	4	Configuration review + sampling	Config export + screenshots	Semi-annual
Detection and alerting	3	Automated control telemetry	Dashboard / telemetry extract	Annual
Log integrity and retention	3	Evidence inspection + interview	Approved records + tickets	Monthly
Detection engineering and threat coverage	4	Re-performance / observation	Observed run + sign-off	Semi-annual
Security operations and response readiness	4	Log and exception review	SIEM / log extract	Annual
Governance, accountability and policy lifecycle	4	Independent test / scan	Scan / test report	Annual
Risk assessment and treatment	4	Configuration review + sampling	Config export + screenshots	Semi-annual

Control area	Ctrls	Test method	Evidence	Frequency
Monitoring, measurement and reporting	4	Automated control telemetry	Dashboard / telemetry extract	Semi-annual
Records, retention and evidence	4	Evidence inspection + interview	Approved records + tickets	Quarterly
Continuous improvement	3	Re-performance / observation	Observed run + sign-off	Quarterly

Evidence is retained for audit per the records-retention schedule and crosswalked to ASD ISM, Essential Eight, ISO/IEC 27001:2022, SOC 2 (TSC), APRA CPS 234.

13. Document approval and distribution

Approval	Name	Role	Date
Prepared by	Nadia Petrova	Privacy Counsel	10 Oct 2026
Reviewed by	Priya Sharma	Chief Information Security Officer	20 Oct 2026
Approved by	Priya Sharma	Chief Information Security Officer	26 Oct 2026
Endorsed by	—	Board Risk Committee	30 Oct 2026

Distribution: all staff and contractors via the policy portal; control owners; Risk & Compliance (2nd line); Internal Audit (3rd line); relevant material service providers under NDA.

14. Abbreviations

Abbreviation	Meaning
ISMS	Information Security Management System
MFA / SSO	Multi-Factor Authentication / Single Sign-On
PAM / IGA	Privileged Access Management / Identity Governance & Administration
RTO / RPO	Recovery Time Objective / Recovery Point Objective
SoD	Segregation of Duties
KRI / KPI	Key Risk Indicator / Key Performance Indicator
SIEM / SOC	Security Information & Event Management / Security Operations Centre

15. Revision history

Version	Date	Author	Summary of change
1.0	03 Oct 2023	Greg Thompson	Initial issue.
2.0	02 Oct 2024	Mei-Lin Tan	Annual review; control uplift and framework alignment.
3.3	02 Oct 2025	Nadia Petrova	Updated for current framework versions and cloud scope.