Southern Mutual Bank

51 824 753 556

AI Decision Review, Contestability & Quality Assurance Procedure

Procedure · synthetic assessor-grade test document

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

Document ID	SOU-PRO-0055
Version	2.0
Owner	Aisha Khan (Security Operations Lead)
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 procedure establishes the requirements, accountabilities and control objectives for ai decision review, contestability & quality assurance procedure across Southern Mutual Bank (“the Bank”). It forms part of the Bank's Information Security Management System and supports its obligations under ISO/IEC 42001, NIST AI RMF, APRA CPS 234. It applies to Core banking platform and supporting services.

Control objectives:

• Govern the responsible, safe and compliant use of AI across its lifecycle.

• Ensure AI systems are inventoried, risk-assessed, monitored and subject to human oversight.

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: ISO/IEC 42001, NIST AI RMF, APRA CPS 234. Where an obligation is more stringent in one framework, the most stringent requirement applies.

4. Requirements

4.1 Inventory and risk classification

4.1.1 AI systems shall be inventoried with owner, purpose, data sources, model/provider, and risk classification.

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. configuration review + sampling. *Frequency.* Monthly. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.1.2 High-risk AI use-cases shall undergo an AI impact assessment before deployment and on material change.

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.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.1.3 AI use affecting customers, credit, fraud or eligibility decisions shall be treated as higher risk by default.

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. re-performance / observation. *Frequency.* Monthly. *Control owner.* Security Operations Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.2 Provider and data governance

4.2.1 AI providers shall be governed for content-filtering, prompt-injection defence, data residency, training opt-out, encryption and logging.

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. configuration review + sampling. *Frequency.* Quarterly. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2.2 Tenant data shall not be used to train provider models unless explicitly approved and contracted.

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.* Semi-annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2.3 Model versions shall be pinned and changes assessed before adoption.

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.* Semi-annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.3 Oversight, evaluation and transparency

4.3.1 Human oversight shall be defined for AI-assisted decisions affecting customers, with the ability to review and override.

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. re-performance / observation. *Frequency.* Semi-annual. *Control owner.* Security Operations Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.3.2 AI outputs shall be evaluated for accuracy, bias/fairness and drift on a defined cadence, with thresholds and actions.

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.* Annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.3.3 Customers shall be informed where they interact with AI, and explainability shall be provided commensurate with risk.

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.* Quarterly. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4 Records of AI decisions, challenges and contestability

4.4.1 Every significant decision informed by an AI system shall be recorded with the inputs, model version, human reviewer and outcome, under the records management framework and the record retention schedule, so that an affected person can challenge a specific decision concerning them.

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.* Security Operations Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.4.2 A documented procedure shall allow an affected AI subject to challenge a specific decision: the challenge, the human review of the decision, the reasons given and the outcome shall be recorded, retained per the record retention schedule and reported quarterly to the AI governance forum.

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.* Semi-annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4.3 Documentation of each AI system — purpose, data sources, model and provider, limitations, evaluation results and the record keeping applied — shall be maintained under document control and made available to assessors and regulators on request.

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. automated telemetry review. *Frequency.* Annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4.4 When an AI system informs a person about significant choices they will make, the options presented shall not be unreasonably restricted and the person's value judgements shall not be influenced without their explicit consent; the consent basis and the options presented shall be recorded.

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.* Quarterly. *Control owner.* Security Operations Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.5 Model lifecycle and validation

4.5.1 AI/ML models shall follow a documented lifecycle: design, data governance, validation, approval, deployment, monitoring and retirement.

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.* Semi-annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5.2 Models shall be independently validated for fitness, accuracy and bias before production and on material change.

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.* Semi-annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5.3 Training and input data shall be governed for quality, lineage, consent and bias.

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. automated telemetry review. *Frequency.* Annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5.4 Model performance and drift shall be monitored against thresholds, with retraining or rollback triggers.

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. configuration review + sampling. *Frequency.* Monthly. *Control owner.* Security Operations Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.6 Generative AI and provider controls

4.6.1 Generative-AI usage shall be approved, inventoried and bounded by acceptable-use and data-handling rules.

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.* Quarterly. *Control owner.* Security Operations Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.6.2 Providers shall be governed for content filtering, prompt-injection defence, training opt-out, data residency and logging.

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.* Quarterly. *Control owner.* Security Operations Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.6.3 Sensitive or regulated data shall not be sent to AI services unless explicitly approved and contractually protected.

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.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.6.4 Outputs used in customer or regulatory contexts shall have human review proportionate to risk.

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.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.7 Governance, accountability and policy lifecycle

4.7.1 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 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. automated telemetry review. *Frequency.* Monthly. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.7.2 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 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.* Quarterly. *Control owner.* Security Operations Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.7.3 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 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.* Annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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.* Security Operations Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.8 Risk assessment and treatment

4.8.1 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 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. automated telemetry review. *Frequency.* Annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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. automated telemetry review. *Frequency.* Annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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.* Semi-annual. *Control owner.* Security Operations Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.9 Monitoring, measurement and reporting

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

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.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.9.2 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 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. configuration review + sampling. *Frequency.* Quarterly. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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. configuration review + sampling. *Frequency.* Annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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.* Quarterly. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.10 Records, retention and evidence

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

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. configuration review + sampling. *Frequency.* Annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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. configuration review + sampling. *Frequency.* Monthly. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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.* Semi-annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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 monitored in the SIEM with detections mapped to the relevant threats.

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

Test method. configuration review + sampling. *Frequency.* Annual. *Control owner.* Security Operations Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.11 Continuous improvement

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

Control objective / rationale. This 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.* Quarterly. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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. automated telemetry review. *Frequency.* Semi-annual. *Control owner.* Security Operations Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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 monitored in the SIEM with detections mapped to the relevant threats.

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

Test method. automated telemetry review. *Frequency.* Quarterly. *Control owner.* Security Operations Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

5. Roles and responsibilities (RACI)

Role	R	A	C	I	Responsibility
Security Operations Lead	✓	✓			Owns this document; ensures it is current, resourced and effective.
System / Asset owners	✓		✓		Implement and operate the controls in their scope.
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 Register every AI use-case; complete an impact assessment for high-risk cases before go-live.

6.2 Assess provider governance posture and contract terms before adoption.

6.3 Monitor accuracy/bias/drift; review with the AI governance forum; act on threshold breaches.

7. Monitoring, metrics and KPIs

Metric	Target	Frequency
AI systems registered with owner + risk class	100%	Quarterly
High-risk AI with current impact assessment	100%	Quarterly
AI systems with drift/bias monitoring	≥ 90%	Monthly
Customer-facing AI with disclosure	100%	Quarterly

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
AI impact assessment	Structured assessment of an AI use-case's risk, including fairness and safety.
Model drift	Degradation of model performance as data or conditions change over time.
Human oversight	A defined human role able to review, approve or override AI-assisted decisions.

11. Related documents

• AI Governance Policy

• AI System Register & Use-Case Inventory

• Risk Management Framework

12. Control framework mapping

Framework	Indicative mapped controls
ISO/IEC 42001	6.1, 8.3, 9.1
NIST AI RMF	GOVERN, MAP, MEASURE, MANAGE
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: Govern the responsible, safe and compliant use of AI across its lifecycle.

• Risk addressed: Ensure AI systems are inventoried, risk-assessed, monitored and subject to human oversight.

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	AI systems shall be inventoried with owner, purpose, data sources, mod…	ISO/IEC 42001	Semi-annual	Implemented
4.1.2	High-risk AI use-cases shall undergo an AI impact assessment before de…	NIST AI RMF	Semi-annual	Implemented
4.1.3	AI use affecting customers, credit, fraud or eligibility decisions sha…	APRA CPS 234	Quarterly	Implemented
4.2.1	AI providers shall be governed for content-filtering, prompt-injection…	ISO/IEC 42001	Annual	Implemented
4.2.2	Tenant data shall not be used to train provider models unless explicit…	NIST AI RMF	Quarterly	Implemented
4.2.3	Model versions shall be pinned and changes assessed before adoption.	APRA CPS 234	Annual	Implemented
4.3.1	Human oversight shall be defined for AI-assisted decisions affecting c…	ISO/IEC 42001	Semi-annual	Partially implemented
4.3.2	AI outputs shall be evaluated for accuracy, bias/fairness and drift on…	NIST AI RMF	Quarterly	Implemented
4.3.3	Customers shall be informed where they interact with AI, and explainab…	APRA CPS 234	Semi-annual	Partially implemented
4.4.1	Every significant decision informed by an AI system shall be recorded …	ISO/IEC 42001	Annual	Implemented
4.4.2	A documented procedure shall allow an affected AI subject to challenge…	NIST AI RMF	Semi-annual	Implemented
4.4.3	Documentation of each AI system — purpose, data sources, model and pro…	APRA CPS 234	Annual	Implemented
4.4.4	When an AI system informs a person about significant choices they will…	ISO/IEC 42001	Monthly	Implemented
4.5.1	AI/ML models shall follow a documented lifecycle: design, data governa…	NIST AI RMF	Monthly	Implemented
4.5.2	Models shall be independently validated for fitness, accuracy and bias…	APRA CPS 234	Quarterly	Implemented
4.5.3	Training and input data shall be governed for quality, lineage, consen…	ISO/IEC 42001	Monthly	Partially implemented
4.5.4	Model performance and drift shall be monitored against thresholds, wit…	NIST AI RMF	Monthly	Partially implemented

Ref	Control statement	Framework	Test freq.	Status
4.6.1	Generative-AI usage shall be approved, inventoried and bounded by acce…	APRA CPS 234	Monthly	Implemented
4.6.2	Providers shall be governed for content filtering, prompt-injection de…	ISO/IEC 42001	Annual	Partially implemented
4.6.3	Sensitive or regulated data shall not be sent to AI services unless ex…	NIST AI RMF	Monthly	Implemented
4.6.4	Outputs used in customer or regulatory contexts shall have human revie…	APRA CPS 234	Quarterly	Implemented
4.7.1	A named executive owner shall be accountable for this control area and…	ISO/IEC 42001	Semi-annual	Partially implemented
4.7.2	This document shall be reviewed at least annually and after any materi…	NIST AI RMF	Annual	Implemented
4.7.3	Roles and responsibilities shall align to the three-lines-of-defence m…	APRA CPS 234	Semi-annual	Implemented
4.7.4	Material decisions, approvals and deviations shall be minuted and reta…	ISO/IEC 42001	Monthly	Implemented
4.8.1	Risks within this control area shall be identified, assessed (likeliho…	NIST AI RMF	Semi-annual	Partially implemented
4.8.2	Residual risk exceeding the approved risk appetite shall be escalated …	APRA CPS 234	Annual	Partially implemented
4.8.3	Risk assessments shall be refreshed on a defined cadence and upon sign…	ISO/IEC 42001	Quarterly	Implemented
4.8.4	Key risk indicators (KRIs) shall be defined and monitored against thre…	NIST AI RMF	Quarterly	Implemented
4.9.1	Control performance shall be monitored continuously through automated …	APRA CPS 234	Semi-annual	Implemented
4.9.2	The metrics and targets in this document shall be reported monthly to …	ISO/IEC 42001	Monthly	Implemented
4.9.3	Control failures and exceptions shall be logged, triaged by severity a…	NIST AI RMF	Annual	Implemented
4.9.4	Independent assurance (internal audit / external assessment) shall per…	APRA CPS 234	Monthly	Implemented
4.10.1	Evidence demonstrating the operation of these controls shall be genera…	ISO/IEC 42001	Monthly	Implemented
4.10.2	Evidence shall be sufficient for an independent assessor to conclude o…	NIST AI RMF	Semi-annual	Implemented
4.10.3	Access to control evidence shall be least-privilege and itself logged;…	APRA CPS 234	Annual	Implemented
4.10.4	On decommissioning, records shall be retained or disposed of per the r…	ISO/IEC 42001	Quarterly	Implemented
4.11.1	Lessons from incidents, audits, assessments and exercises shall be fed…	NIST AI RMF	Semi-annual	Implemented
4.11.2	Control maturity shall be assessed against a defined target state, wit…	APRA CPS 234	Quarterly	Implemented
4.11.3	Automation and tooling shall be progressively adopted to reduce manual…	ISO/IEC 42001	Annual	Implemented

Appendix A — Control implementation checklist

Control area	Controls	Implementation status
Inventory and risk classification	3 control(s)	Implemented
Provider and data governance	3 control(s)	Implemented
Oversight, evaluation and transparency	3 control(s)	Planned
Records of AI decisions, challenges and contestability	4 control(s)	Partially implemented
Model lifecycle and validation	4 control(s)	Implemented
Generative AI and provider controls	4 control(s)	Implemented
Governance, accountability and policy lifecycle	4 control(s)	Implemented
Risk assessment and treatment	4 control(s)	Implemented
Monitoring, measurement and reporting	4 control(s)	Implemented
Records, retention and evidence	4 control(s)	Partially implemented
Continuous improvement	3 control(s)	Partially implemented

Appendix B — Control testing and evidence matrix

Control area	Ctrls	Test method	Evidence	Frequency
Inventory and risk classification	3	Configuration review + sampling	Config export + screenshots	Monthly
Provider and data governance	3	Automated control telemetry	Dashboard / telemetry extract	Quarterly
Oversight, evaluation and transparency	3	Evidence inspection + interview	Approved records + tickets	Monthly
Records of AI decisions, challenges and contestability	4	Re-performance / observation	Observed run + sign-off	Annual
Model lifecycle and validation	4	Log and exception review	SIEM / log extract	Annual
Generative AI and provider controls	4	Independent test / scan	Scan / test report	Quarterly
Governance, accountability and policy lifecycle	4	Configuration review + sampling	Config export + screenshots	Quarterly
Risk assessment and treatment	4	Automated control telemetry	Dashboard / telemetry extract	Semi-annual
Monitoring, measurement and reporting	4	Evidence inspection + interview	Approved records + tickets	Monthly
Records, retention and evidence	4	Re-performance / observation	Observed run + sign-off	Semi-annual
Continuous improvement	3	Log and exception review	SIEM / log extract	Monthly

Evidence is retained for audit per the records-retention schedule and crosswalked to ISO/IEC 42001, NIST AI RMF, APRA CPS 234.

13. Document approval and distribution

Approval	Name	Role	Date
Prepared by	Aisha Khan	Security Operations Lead	10 Oct 2026
Reviewed by	Nadia Petrova	Privacy Counsel	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 2024	Laura Mendez	Initial issue.
2.0	02 Oct 2025	Daniel Wright	Annual review; control uplift and framework alignment.