Southern Mutual Bank

51 824 753 556

Privacy Policy

Policy · synthetic assessor-grade test document

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

Document ID	SOU-POL-0022
Version	2.2
Owner	James O'Connor (Head of Operational Risk)
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 privacy policy across Southern Mutual Bank (“the Bank”). It forms part of the Bank's Information Security Management System and supports its obligations under NDB Scheme, APRA CPS 234, ISO/IEC 27001:2022. It applies to Core banking platform and supporting services.

Control objectives:

• Protect personal information across its lifecycle and uphold individuals' privacy rights.

• Meet obligations under the Privacy Act and the Notifiable Data Breaches scheme.

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: NDB Scheme, APRA CPS 234, ISO/IEC 27001:2022. Where an obligation is more stringent in one framework, the most stringent requirement applies.

4. Requirements

4.1 Collection, use and disclosure

4.1.1 Personal information shall be collected, used and disclosed only for lawful, disclosed purposes and minimised to what is necessary.

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.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.1.2 Privacy notices shall be clear, current and provided at the point of collection.

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.* Annual. *Control owner.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.1.3 Cross-border disclosures shall be assessed and controlled per the privacy framework.

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.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2 Rights, retention and disposal

4.2.1 Individuals' rights to access and correction shall be supported through defined, timely processes.

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. automated telemetry review. *Frequency.* Quarterly. *Control owner.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2.2 Retention and disposal of personal information shall follow the records-retention schedule; over-retention is prohibited.

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.* Head of Operational Risk. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.2.3 Personal information shall be classified and handled per the data classification standard.

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.* Quarterly. *Control owner.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.3 Privacy by design and breaches

4.3.1 Privacy impact assessments (PIA) shall be completed for new or materially changed processing.

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.* Annual. *Control owner.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.3.2 Data flows involving personal information shall be mapped, minimised and reviewed.

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.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.3.3 Eligible data breaches shall be assessed and notified under the NDB scheme within required timeframes.

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.* Quarterly. *Control owner.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4 Consent, collection and minimisation

4.4.1 Personal information shall be collected with a lawful basis and minimised to what is necessary for the disclosed purpose.

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.* Quarterly. *Control owner.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4.2 Consent, where relied upon, shall be informed, specific and withdrawable, and records maintained.

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.* Monthly. *Control owner.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4.3 Secondary use and disclosure shall be assessed against the original purpose and privacy framework.

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.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4.4 De-identification and pseudonymisation shall be applied where it reduces privacy risk without defeating the purpose.

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.* Quarterly. *Control owner.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5 Cross-border transfers and data residency

4.5.1 Cross-border disclosures of personal information shall be assessed and controlled, with accountability for overseas recipients.

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. configuration review + sampling. *Frequency.* Annual. *Control owner.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5.2 Data residency requirements shall be defined per data class and enforced in cloud configuration.

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. configuration review + sampling. *Frequency.* Monthly. *Control owner.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5.3 Transfer mechanisms and contractual protections shall be documented for overseas processing.

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.* Annual. *Control owner.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5.4 Data-flow maps shall identify all cross-border flows of personal information.

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.* Semi-annual. *Control owner.* Head of Operational Risk. *Status.* 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. automated telemetry review. *Frequency.* Semi-annual. *Control owner.* Head of Operational Risk. *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. automated telemetry review. *Frequency.* Semi-annual. *Control owner.* Head of Operational Risk. *Status.* Partially 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.* Semi-annual. *Control owner.* Head of Operational Risk. *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. automated telemetry review. *Frequency.* Annual. *Control owner.* Head of Operational Risk. *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. configuration review + sampling. *Frequency.* Monthly. *Control owner.* Head of Operational Risk. *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. re-performance / observation. *Frequency.* Annual. *Control owner.* Head of Operational Risk. *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. automated telemetry review. *Frequency.* Semi-annual. *Control owner.* Head of Operational Risk. *Status.* 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. automated telemetry review. *Frequency.* Semi-annual. *Control owner.* Head of Operational Risk. *Status.* 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. configuration review + sampling. *Frequency.* Semi-annual. *Control owner.* Head of Operational Risk. *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. automated telemetry review. *Frequency.* Monthly. *Control owner.* Head of Operational Risk. *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. log + exception review. *Frequency.* Monthly. *Control owner.* Head of Operational Risk. *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. log + exception review. *Frequency.* Annual. *Control owner.* Head of Operational Risk. *Status.* 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.* Monthly. *Control owner.* Head of Operational Risk. *Status.* Partially 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. log + exception review. *Frequency.* Quarterly. *Control owner.* Head of Operational Risk. *Status.* 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. log + exception review. *Frequency.* Quarterly. *Control owner.* Head of Operational Risk. *Status.* Partially 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. automated telemetry review. *Frequency.* Annual. *Control owner.* Head of Operational Risk. *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.* Head of Operational Risk. *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.* Quarterly. *Control owner.* Head of Operational Risk. *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. automated telemetry review. *Frequency.* Quarterly. *Control owner.* Head of Operational Risk. *Status.* Partially implemented (self-declared by the document author; not independently verified).

5. Roles and responsibilities (RACI)

Role	R	A	C	I	Responsibility
Head of Operational Risk	✓	✓			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 Complete a PIA for new processing; record outcomes and controls.

6.2 Operate access/correction request handling within statutory timeframes.

6.3 Assess suspected breaches with Legal/Privacy; notify the OAIC and individuals where required.

7. Monitoring, metrics and KPIs

Metric	Target	Frequency
PIAs completed for in-scope changes	100%	Quarterly
Access/correction requests within SLA	≥ 95%	Monthly
Eligible breaches notified within window	100%	Per incident
Records beyond retention disposed	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
Personal information	Information about an identified or reasonably identifiable individual.
PIA	Privacy Impact Assessment — structured assessment of privacy risk.
Eligible data breach	A breach likely to result in serious harm, triggering NDB notification.

11. Related documents

- Privacy Policy
- Data Retention & Disposal Standard
- Data Breach Response Procedure

12. Control framework mapping

Framework	Indicative mapped controls
NDB Scheme	Assessment, Notification
APRA CPS 234	Information security capability, Control testing, Incident notification
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23

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: Protect personal information across its lifecycle and uphold individuals' privacy rights.
- Risk addressed: Meet obligations under the Privacy Act and the Notifiable Data Breaches scheme.

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	Personal information shall be collected, used and disclosed only for l…	NDB Scheme	Semi-annual	Implemented
4.1.2	Privacy notices shall be clear, current and provided at the point of c…	APRA CPS 234	Semi-annual	Implemented
4.1.3	Cross-border disclosures shall be assessed and controlled per the priv…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.2.1	Individuals' rights to access and correction shall be supported throug…	NDB Scheme	Annual	Implemented
4.2.2	Retention and disposal of personal information shall follow the record…	APRA CPS 234	Annual	Partially implemented
4.2.3	Personal information shall be classified and handled per the data clas…	ISO/IEC 27001:2022	Annual	Partially implemented
4.3.1	Privacy impact assessments (PIA) shall be completed for new or materia…	NDB Scheme	Monthly	Implemented
4.3.2	Data flows involving personal information shall be mapped, minimised a…	APRA CPS 234	Semi-annual	Partially implemented
4.3.3	Eligible data breaches shall be assessed and notified under the NDB sc…	ISO/IEC 27001:2022	Monthly	Partially implemented
4.4.1	Personal information shall be collected with a lawful basis and minimi…	NDB Scheme	Semi-annual	Implemented
4.4.2	Consent, where relied upon, shall be informed, specific and withdrawab…	APRA CPS 234	Monthly	Implemented
4.4.3	Secondary use and disclosure shall be assessed against the original pu…	ISO/IEC 27001:2022	Monthly	Implemented
4.4.4	De-identification and pseudonymisation shall be applied where it reduc…	NDB Scheme	Monthly	Implemented
4.5.1	Cross-border disclosures of personal information shall be assessed and…	APRA CPS 234	Quarterly	Partially implemented
4.5.2	Data residency requirements shall be defined per data class and enforc…	ISO/IEC 27001:2022	Annual	Implemented
4.5.3	Transfer mechanisms and contractual protections shall be documented fo…	NDB Scheme	Semi-annual	Partially implemented
4.5.4	Data-flow maps shall identify all cross-border flows of personal infor…	APRA CPS 234	Semi-annual	Implemented

Ref	Control statement	Framework	Test freq.	Status
4.6.1	A named executive owner shall be accountable for this control area and…	ISO/IEC 27001:2022	Monthly	Implemented
4.6.2	This document shall be reviewed at least annually and after any materi…	NDB Scheme	Annual	Partially implemented
4.6.3	Roles and responsibilities shall align to the three-lines-of-defence m…	APRA CPS 234	Monthly	Partially implemented
4.6.4	Material decisions, approvals and deviations shall be minuted and reta…	ISO/IEC 27001:2022	Annual	Implemented
4.7.1	Risks within this control area shall be identified, assessed (likeliho…	NDB Scheme	Monthly	Implemented
4.7.2	Residual risk exceeding the approved risk appetite shall be escalated …	APRA CPS 234	Semi-annual	Implemented
4.7.3	Risk assessments shall be refreshed on a defined cadence and upon sign…	ISO/IEC 27001:2022	Monthly	Partially implemented
4.7.4	Key risk indicators (KRIs) shall be defined and monitored against thre…	NDB Scheme	Semi-annual	Partially implemented
4.8.1	Control performance shall be monitored continuously through automated …	APRA CPS 234	Annual	Implemented
4.8.2	The metrics and targets in this document shall be reported monthly to …	ISO/IEC 27001:2022	Monthly	Partially implemented
4.8.3	Control failures and exceptions shall be logged, triaged by severity a…	NDB Scheme	Annual	Implemented
4.8.4	Independent assurance (internal audit / external assessment) shall per…	APRA CPS 234	Monthly	Implemented
4.9.1	Evidence demonstrating the operation of these controls shall be genera…	ISO/IEC 27001:2022	Annual	Implemented
4.9.2	Evidence shall be sufficient for an independent assessor to conclude o…	NDB Scheme	Monthly	Partially implemented
4.9.3	Access to control evidence shall be least-privilege and itself logged;…	APRA CPS 234	Annual	Implemented
4.9.4	On decommissioning, records shall be retained or disposed of per the r…	ISO/IEC 27001:2022	Annual	Implemented
4.10.1	Lessons from incidents, audits, assessments and exercises shall be fed…	NDB Scheme	Monthly	Partially implemented
4.10.2	Control maturity shall be assessed against a defined target state, wit…	APRA CPS 234	Semi-annual	Partially implemented
4.10.3	Automation and tooling shall be progressively adopted to reduce manual…	ISO/IEC 27001:2022	Semi-annual	Implemented

Appendix A — Control implementation checklist

Control area	Controls	Implementation status
Collection, use and disclosure	3 control(s)	Planned
Rights, retention and disposal	3 control(s)	Partially implemented
Privacy by design and breaches	3 control(s)	Partially implemented

Control area	Controls	Implementation status
Consent, collection and minimisation	4 control(s)	Implemented
Cross-border transfers and data residency	4 control(s)	Implemented
Governance, accountability and policy lifecycle	4 control(s)	Planned
Risk assessment and treatment	4 control(s)	Implemented
Monitoring, measurement and reporting	4 control(s)	Partially implemented
Records, retention and evidence	4 control(s)	Implemented
Continuous improvement	3 control(s)	Partially implemented

Appendix B — Control testing and evidence matrix

Control area	Ctrls	Test method	Evidence	Frequency
Collection, use and disclosure	3	Configuration review + sampling	Config export + screenshots	Quarterly
Rights, retention and disposal	3	Automated control telemetry	Dashboard / telemetry extract	Annual
Privacy by design and breaches	3	Evidence inspection + interview	Approved records + tickets	Quarterly
Consent, collection and minimisation	4	Re-performance / observation	Observed run + sign-off	Semi-annual
Cross-border transfers and data residency	4	Log and exception review	SIEM / log extract	Quarterly
Governance, accountability and policy lifecycle	4	Independent test / scan	Scan / test report	Annual
Risk assessment and treatment	4	Configuration review + sampling	Config export + screenshots	Annual
Monitoring, measurement and reporting	4	Automated control telemetry	Dashboard / telemetry extract	Quarterly
Records, retention and evidence	4	Evidence inspection + interview	Approved records + tickets	Monthly
Continuous improvement	3	Re-performance / observation	Observed run + sign-off	Quarterly

Evidence is retained for audit per the records-retention schedule and crosswalked to NDB Scheme, APRA CPS 234, ISO/IEC 27001:2022.

13. Document approval and distribution

Approval	Name	Role	Date
Prepared by	James O'Connor	Head of Operational Risk	10 Oct 2026
Reviewed by	Aisha Khan	Security Operations Lead	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

Abbreviation	Meaning
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	David Okafor	Initial issue.
2.2	02 Oct 2025	Tom Bauer	Annual review; control uplift and framework alignment.