Southern Mutual Bank

51 824 753 556

Encryption Standard

Standard · synthetic assessor-grade test document

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

Document ID	SOU-STD-0007
Version	2.2
Owner	Daniel Wright (Business Continuity Manager)
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 standard establishes the requirements, accountabilities and control objectives for encryption standard 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:

• Protect the confidentiality and integrity of information in transit and at rest using approved cryptography.

• Ensure cryptographic keys are generated, stored, rotated and destroyed under controlled key management.

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 Cryptographic standards

4.1.1 Information in transit shall be protected with TLS 1.2 or higher using approved cipher suites; deprecated protocols (SSLv3, TLS 1.0/1.1) shall be removed from service.

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

4.1.2 Information at rest shall be encrypted using AES-256 (or an approved equivalent) across databases, object storage, backups and removable media.

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.* Annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.1.3 Only algorithms and key lengths on the approved cryptographic standard shall be used; bespoke or unvetted cryptography 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. re-performance / observation. *Frequency.* Semi-annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.1.4 Public-facing services shall be assessed against the cryptographic configuration baseline at least quarterly.

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. re-performance / observation. *Frequency.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2 Key management

4.2.1 Cryptographic keys shall be generated and stored within an approved key-management service (KMS) or hardware security module (HSM).

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.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2.2 Customer-managed keys (CMK) shall be used for material data stores where the platform supports them.

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. automated telemetry review. *Frequency.* Semi-annual. *Control owner.* Business Continuity Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.2.3 Keys shall be rotated at least annually and immediately on suspected compromise, with old key versions retained only for decryption of legacy data.

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.* Business Continuity Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.2.4 Key administration shall enforce dual control and split knowledge; no single administrator may export or recover a production key alone.

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.* Monthly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.3 Certificate management

4.3.1 All TLS certificates shall be inventoried with owner, issuer, expiry and the service they protect.

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.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.3.2 Certificate expiry shall be monitored with alerting at 30, 14 and 7 days; auto-renewal shall be used where available.

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.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.3.3 Private keys for certificates shall be stored in the KMS/HSM and never distributed in plaintext.

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.* Monthly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4 PKI and certificate authority governance

4.4.1 Internal and external certificate authorities shall be governed with documented certificate policies and practice statements.

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.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4.2 Certificate issuance shall be authorised, logged and scoped to least privilege; wildcard and long-lived certificates shall be minimised.

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.* Annual. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4.3 Root and intermediate CA keys shall be held in an HSM under dual control with strict physical and logical protection.

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.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4.4 Certificate revocation (CRL/OCSP) shall be operational and monitored.

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.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5 Cryptographic agility and deprecation

4.5.1 An inventory of cryptographic usage shall be maintained to enable rapid response to algorithm deprecation or compromise.

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.* Monthly. *Control owner.* Business Continuity Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.5.2 Deprecated algorithms and protocols shall be removed on a defined timeline; exceptions shall be risk-accepted and time-bound.

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.* Quarterly. *Control owner.* Business Continuity Manager. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5.3 The organisation shall monitor cryptographic standards (incl. post-quantum guidance) and plan migrations accordingly.

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.* Business Continuity Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.5.4 Cryptographic changes shall be tested for interoperability before production rollout.

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

5. Roles and responsibilities (RACI)

Role	R	A	C	I	Responsibility
Business Continuity Manager	✓	✓			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 New services request keys/certificates via the platform team; keys are provisioned in the KMS/HSM.

6.2 Automated jobs scan endpoints for protocol/cipher compliance and certificate expiry.

6.3 Annual key-rotation runbook is executed and evidenced; emergency rotation follows the incident process.

7. Monitoring, metrics and KPIs

Metric	Target	Frequency
Material data stores encrypted at rest	100%	Monthly
Internet-facing endpoints on approved TLS	100%	Monthly
Certificates renewed before expiry	100%	Monthly
Keys rotated within policy period	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
KMS / HSM	A managed service or hardware device that securely generates and stores cryptographic keys.
Customer-managed key (CMK)	An encryption key the organisation controls rather than the provider.
Dual control	A requirement that two authorised people are needed to perform a sensitive action.

11. Related documents

• Information Security Policy

• Encryption Standard

• Data Classification & Handling Standard

12. Control framework mapping

Framework	Indicative mapped controls
ASD ISM	Guidelines: Access, System hardening, Monitoring
Essential Eight	ML2 target
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: Protect the confidentiality and integrity of information in transit and at rest using approved cryptography.

• Risk addressed: Ensure cryptographic keys are generated, stored, rotated and destroyed under controlled key management.

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	Information in transit shall be protected with TLS 1.2 or higher using…	ASD ISM	Monthly	Implemented
4.1.2	Information at rest shall be encrypted using AES-256 (or an approved e…	Essential Eight	Semi-annual	Implemented
4.1.3	Only algorithms and key lengths on the approved cryptographic standard…	ISO/IEC 27001:2022	Annual	Implemented
4.1.4	Public-facing services shall be assessed against the cryptographic con…	SOC 2 (TSC)	Monthly	Implemented

Ref	Control statement	Framework	Test freq.	Status
4.2.1	Cryptographic keys shall be generated and stored within an approved ke…	APRA CPS 234	Quarterly	Partially implemented
4.2.2	Customer-managed keys (CMK) shall be used for material data stores whe…	ASD ISM	Annual	Implemented
4.2.3	Keys shall be rotated at least annually and immediately on suspected c…	Essential Eight	Monthly	Partially implemented
4.2.4	Key administration shall enforce dual control and split knowledge; no …	ISO/IEC 27001:2022	Annual	Partially implemented
4.3.1	All TLS certificates shall be inventoried with owner, issuer, expiry a…	SOC 2 (TSC)	Semi-annual	Implemented
4.3.2	Certificate expiry shall be monitored with alerting at 30, 14 and 7 da…	APRA CPS 234	Monthly	Implemented
4.3.3	Private keys for certificates shall be stored in the KMS/HSM and never…	ASD ISM	Annual	Partially implemented
4.4.1	Internal and external certificate authorities shall be governed with d…	Essential Eight	Semi-annual	Implemented
4.4.2	Certificate issuance shall be authorised, logged and scoped to least p…	ISO/IEC 27001:2022	Monthly	Implemented
4.4.3	Root and intermediate CA keys shall be held in an HSM under dual contr…	SOC 2 (TSC)	Annual	Implemented
4.4.4	Certificate revocation (CRL/OCSP) shall be operational and monitored.	APRA CPS 234	Annual	Partially implemented
4.5.1	An inventory of cryptographic usage shall be maintained to enable rapi…	ASD ISM	Annual	Implemented
4.5.2	Deprecated algorithms and protocols shall be removed on a defined time…	Essential Eight	Quarterly	Implemented
4.5.3	The organisation shall monitor cryptographic standards (incl. post-qua…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.5.4	Cryptographic changes shall be tested for interoperability before prod…	SOC 2 (TSC)	Semi-annual	Implemented
4.6.1	A named executive owner shall be accountable for this control area and…	APRA CPS 234	Monthly	Partially implemented
4.6.2	This document shall be reviewed at least annually and after any materi…	ASD ISM	Quarterly	Implemented
4.6.3	Roles and responsibilities shall align to the three-lines-of-defence m…	Essential Eight	Monthly	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…	SOC 2 (TSC)	Monthly	Implemented
4.7.2	Residual risk exceeding the approved risk appetite shall be escalated …	APRA CPS 234	Monthly	Implemented
4.7.3	Risk assessments shall be refreshed on a defined cadence and upon sign…	ASD ISM	Quarterly	Implemented
4.7.4	Key risk indicators (KRIs) shall be defined and monitored against thre…	Essential Eight	Semi-annual	Implemented

Ref	Control statement	Framework	Test freq.	Status
4.8.1	Control performance shall be monitored continuously through automated …	ISO/IEC 27001:2022	Monthly	Implemented
4.8.2	The metrics and targets in this document shall be reported monthly to …	SOC 2 (TSC)	Annual	Implemented
4.8.3	Control failures and exceptions shall be logged, triaged by severity a…	APRA CPS 234	Annual	Implemented
4.8.4	Independent assurance (internal audit / external assessment) shall per…	ASD ISM	Semi-annual	Implemented
4.9.1	Evidence demonstrating the operation of these controls shall be genera…	Essential Eight	Semi-annual	Implemented
4.9.2	Evidence shall be sufficient for an independent assessor to conclude o…	ISO/IEC 27001:2022	Monthly	Implemented
4.9.3	Access to control evidence shall be least-privilege and itself logged;…	SOC 2 (TSC)	Monthly	Implemented
4.9.4	On decommissioning, records shall be retained or disposed of per the r…	APRA CPS 234	Quarterly	Partially implemented
4.10.1	Lessons from incidents, audits, assessments and exercises shall be fed…	ASD ISM	Monthly	Implemented
4.10.2	Control maturity shall be assessed against a defined target state, wit…	Essential Eight	Semi-annual	Implemented
4.10.3	Automation and tooling shall be progressively adopted to reduce manual…	ISO/IEC 27001:2022	Annual	Partially implemented

Appendix A — Control implementation checklist

Control area	Controls	Implementation status
Cryptographic standards	4 control(s)	Implemented
Key management	4 control(s)	Implemented
Certificate management	3 control(s)	Implemented
PKI and certificate authority governance	4 control(s)	Implemented
Cryptographic agility and deprecation	4 control(s)	Implemented
Governance, accountability and policy lifecycle	4 control(s)	Implemented
Risk assessment and treatment	4 control(s)	Partially 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
Cryptographic standards	4	Configuration review + sampling	Config export + screenshots	Annual
Key management	4	Automated control telemetry	Dashboard / telemetry extract	Quarterly
Certificate management	3	Evidence inspection + interview	Approved records + tickets	Monthly
PKI and certificate authority governance	4	Re-performance / observation	Observed run + sign-off	Quarterly

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

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	Daniel Wright	Business Continuity Manager	10 Oct 2026
Reviewed by	Mei-Lin Tan	IT Operations Manager	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	Nadia Petrova	Initial issue.
2.2	02 Oct 2025	Greg Thompson	Annual review; control uplift and framework alignment.