Southern Mutual Bank

51 824 753 556

Secure System Build & Hardening Procedure

Procedure · synthetic assessor-grade test document

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

Document ID	SOU-PRO-0050
Version	3.0
Owner	Mei-Lin Tan (IT Operations 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 procedure establishes the requirements, accountabilities and control objectives for secure system build & hardening procedure 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:

• Reduce exposure by identifying and remediating vulnerabilities and misconfigurations within risk-based timeframes.

• Maintain systems on supported, securely configured versions.

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 Vulnerability identification

4.1.1 Authenticated vulnerability scanning shall be performed at least monthly across the estate; internet-facing assets weekly.

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

4.1.2 Threat intelligence shall be used to prioritise actively-exploited vulnerabilities.

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

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

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

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

4.1.3 Penetration testing shall be performed at least annually and after material change to internet-facing services.

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

4.2 Remediation timeframes

4.2.1 Critical vulnerabilities shall be remediated within 48 hours, high within 14 days, medium within 30 days, low within 90 days.

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

4.2.2 Where remediation is not feasible in time, a documented risk acceptance with compensating controls shall be recorded and time-bound.

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

4.2.3 End-of-life software shall be removed, upgraded or isolated with compensating controls.

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

4.3 Secure configuration and change

4.3.1 Secure configuration baselines (e.g. CIS-aligned) shall be applied to operating systems, databases and cloud services, and drift monitored.

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

4.3.2 Changes shall be authorised, tested and recorded before deployment to production via the change process.

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

4.3.3 Internet-facing services shall be hardened and reviewed against the configuration standard.

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

4.4 Vulnerability prioritisation and SLAs

4.4.1 Vulnerabilities shall be prioritised using severity and exploitability (e.g. CVSS + known-exploited intelligence).

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

4.4.2 Remediation SLAs shall be defined by severity and asset exposure, and breaches escalated.

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

4.4.3 Compensating controls shall be applied and risk-accepted where remediation cannot meet the SLA.

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

4.4.4 Vulnerability metrics (open criticals, mean-time-to-remediate) shall be reported to risk governance.

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

4.5 Cloud, container and pipeline hardening

4.5.1 Cloud configurations shall be assessed continuously against secure baselines (e.g. CIS benchmarks) with drift remediated.

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

4.5.2 Container images shall be scanned for vulnerabilities and signed; only approved base images shall be used.

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

4.5.3 Infrastructure-as-code shall be scanned for misconfiguration before deployment.

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

4.5.4 CI/CD pipelines shall enforce security gates and least-privilege service credentials.

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

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

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

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

4.6 Governance, accountability and policy lifecycle

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

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

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

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

Test method. log + exception review. *Frequency.* Monthly. *Control owner.* IT Operations 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.* Monthly. *Control owner.* IT Operations 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. configuration review + sampling. *Frequency.* Semi-annual. *Control owner.* IT Operations 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. automated telemetry review. *Frequency.* Semi-annual. *Control owner.* IT Operations 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. log + exception review. *Frequency.* Annual. *Control owner.* IT Operations 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. configuration review + sampling. *Frequency.* Quarterly. *Control owner.* IT Operations 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. automated telemetry review. *Frequency.* Annual. *Control owner.* IT Operations Manager. *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. log + exception review. *Frequency.* Semi-annual. *Control owner.* IT Operations 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. automated telemetry review. *Frequency.* Annual. *Control owner.* IT Operations 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.* Semi-annual. *Control owner.* IT Operations Manager. *Status.* Partially 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. automated telemetry review. *Frequency.* Semi-annual. *Control owner.* IT Operations 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.* Quarterly. *Control owner.* IT Operations Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.9 Records, retention and evidence

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

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

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

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

Test method. re-performance / observation. *Frequency.* Monthly. *Control owner.* IT Operations 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. re-performance / observation. *Frequency.* Quarterly. *Control owner.* IT Operations 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. configuration review + sampling. *Frequency.* Semi-annual. *Control owner.* IT Operations 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. re-performance / observation. *Frequency.* Monthly. *Control owner.* IT Operations 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. configuration review + sampling. *Frequency.* Semi-annual. *Control owner.* IT Operations 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.* Quarterly. *Control owner.* IT Operations 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.* Annual. *Control owner.* IT Operations Manager. *Status.* Partially implemented (self-declared by the document author; not independently verified).

5. Roles and responsibilities (RACI)

Role	R	A	C	I	Responsibility
IT Operations 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 Scanners run on schedule; findings flow to owners via the vulnerability-management platform with SLAs.

6.2 Patch cycles are planned and deployed through change management; emergency patches follow the expedited path.

6.3 Configuration baselines are enforced via tooling; drift generates remediation tickets.

7. Monitoring, metrics and KPIs

Metric	Target	Frequency
Critical vulnerabilities remediated ≤ 48h	≥ 95%	Monthly
Estate patched to supported versions	≥ 98%	Monthly
Assets on approved secure baseline	≥ 95%	Monthly
End-of-life systems without compensating control	0	Monthly

8. Compliance, monitoring and enforcement

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

9. Exceptions and waivers

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

10. Definitions

Term	Definition
CVSS	Common Vulnerability Scoring System — severity rating for vulnerabilities.
Configuration drift	Deviation of a system's settings from its approved secure baseline.
Risk acceptance	A documented, time-bound decision to tolerate a residual risk with compensating controls.

11. Related documents

- Patch Management Standard
- Secure Configuration Baseline Standard
- Change Management Policy

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: Reduce exposure by identifying and remediating vulnerabilities and misconfigurations within risk-based timeframes.

• Risk addressed: Maintain systems on supported, securely configured versions.

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	Authenticated vulnerability scanning shall be performed at least month…	ASD ISM	Quarterly	Implemented
4.1.2	Threat intelligence shall be used to prioritise actively-exploited vul…	Essential Eight	Annual	Partially implemented
4.1.3	Penetration testing shall be performed at least annually and after mat…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.2.1	Critical vulnerabilities shall be remediated within 48 hours, high wit…	SOC 2 (TSC)	Quarterly	Implemented
4.2.2	Where remediation is not feasible in time, a documented risk acceptanc…	APRA CPS 234	Monthly	Implemented
4.2.3	End-of-life software shall be removed, upgraded or isolated with compe…	ASD ISM	Quarterly	Implemented
4.3.1	Secure configuration baselines (e.g. CIS-aligned) shall be applied to …	Essential Eight	Quarterly	Implemented
4.3.2	Changes shall be authorised, tested and recorded before deployment to …	ISO/IEC 27001:2022	Annual	Implemented
4.3.3	Internet-facing services shall be hardened and reviewed against the co…	SOC 2 (TSC)	Monthly	Implemented
4.4.1	Vulnerabilities shall be prioritised using severity and exploitability…	APRA CPS 234	Monthly	Implemented
4.4.2	Remediation SLAs shall be defined by severity and asset exposure, and …	ASD ISM	Quarterly	Implemented
4.4.3	Compensating controls shall be applied and risk-accepted where remedia…	Essential Eight	Semi-annual	Implemented
4.4.4	Vulnerability metrics (open criticals, mean-time-to-remediate) shall b…	ISO/IEC 27001:2022	Quarterly	Implemented
4.5.1	Cloud configurations shall be assessed continuously against secure bas…	SOC 2 (TSC)	Semi-annual	Implemented

Ref	Control statement	Framework	Test freq.	Status
4.5.2	Container images shall be scanned for vulnerabilities and signed; only…	APRA CPS 234	Semi-annual	Implemented
4.5.3	Infrastructure-as-code shall be scanned for misconfiguration before de…	ASD ISM	Quarterly	Partially implemented
4.5.4	CI/CD pipelines shall enforce security gates and least-privilege servi…	Essential Eight	Quarterly	Partially implemented
4.6.1	A named executive owner shall be accountable for this control area and…	ISO/IEC 27001:2022	Annual	Implemented
4.6.2	This document shall be reviewed at least annually and after any materi…	SOC 2 (TSC)	Annual	Partially implemented
4.6.3	Roles and responsibilities shall align to the three-lines-of-defence m…	APRA CPS 234	Quarterly	Implemented
4.6.4	Material decisions, approvals and deviations shall be minuted and reta…	ASD ISM	Semi-annual	Implemented
4.7.1	Risks within this control area shall be identified, assessed (likeliho…	Essential Eight	Annual	Implemented
4.7.2	Residual risk exceeding the approved risk appetite shall be escalated …	ISO/IEC 27001:2022	Semi-annual	Implemented
4.7.3	Risk assessments shall be refreshed on a defined cadence and upon sign…	SOC 2 (TSC)	Quarterly	Implemented
4.7.4	Key risk indicators (KRIs) shall be defined and monitored against thre…	APRA CPS 234	Semi-annual	Implemented
4.8.1	Control performance shall be monitored continuously through automated …	ASD ISM	Semi-annual	Implemented
4.8.2	The metrics and targets in this document shall be reported monthly to …	Essential Eight	Semi-annual	Implemented
4.8.3	Control failures and exceptions shall be logged, triaged by severity a…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.8.4	Independent assurance (internal audit / external assessment) shall per…	SOC 2 (TSC)	Semi-annual	Partially implemented
4.9.1	Evidence demonstrating the operation of these controls shall be genera…	APRA CPS 234	Semi-annual	Implemented
4.9.2	Evidence shall be sufficient for an independent assessor to conclude o…	ASD ISM	Monthly	Partially implemented
4.9.3	Access to control evidence shall be least-privilege and itself logged;…	Essential Eight	Annual	Implemented
4.9.4	On decommissioning, records shall be retained or disposed of per the r…	ISO/IEC 27001:2022	Annual	Partially implemented
4.10.1	Lessons from incidents, audits, assessments and exercises shall be fed…	SOC 2 (TSC)	Annual	Implemented
4.10.2	Control maturity shall be assessed against a defined target state, wit…	APRA CPS 234	Semi-annual	Implemented
4.10.3	Automation and tooling shall be progressively adopted to reduce manual…	ASD ISM	Semi-annual	Implemented

Appendix A — Control implementation checklist

Control area	Controls	Implementation status
Vulnerability identification	3 control(s)	Implemented
Remediation timeframes	3 control(s)	Planned
Secure configuration and change	3 control(s)	Implemented
Vulnerability prioritisation and SLAs	4 control(s)	Partially implemented
Cloud, container and pipeline hardening	4 control(s)	Planned
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)	Implemented

Appendix B — Control testing and evidence matrix

Control area	Ctrls	Test method	Evidence	Frequency
Vulnerability identification	3	Configuration review + sampling	Config export + screenshots	Annual
Remediation timeframes	3	Automated control telemetry	Dashboard / telemetry extract	Semi-annual
Secure configuration and change	3	Evidence inspection + interview	Approved records + tickets	Semi-annual
Vulnerability prioritisation and SLAs	4	Re-performance / observation	Observed run + sign-off	Monthly
Cloud, container and pipeline hardening	4	Log and exception review	SIEM / log extract	Monthly
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	Annual
Records, retention and evidence	4	Evidence inspection + interview	Approved records + tickets	Monthly
Continuous improvement	3	Re-performance / observation	Observed run + sign-off	Semi-annual

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	Mei-Lin Tan	IT Operations Manager	10 Oct 2026
Reviewed by	David Okafor	Head of Compliance	20 Oct 2026
Approved by	Priya Sharma	Chief Information Security Officer	26 Oct 2026
Endorsed by	—	Board Risk Committee	30 Oct 2026

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

14. Abbreviations

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

15. Revision history

Version	Date	Author	Summary of change
1.0	03 Oct 2023	Priya Sharma	Initial issue.
2.0	02 Oct 2024	James O'Connor	Annual review; control uplift and framework alignment.
3.0	02 Oct 2025	Mei-Lin Tan	Updated for current framework versions and cloud scope.