Southern Mutual Bank

51 824 753 556

Security Testing & Assurance Procedure

Procedure · synthetic assessor-grade test document

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

Document ID	SOU-PRO-0053
Version	3.3
Owner	David Okafor (Head of Compliance)
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 security testing & assurance 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:

• Build security into the software development lifecycle (SDLC) so applications are secure by design and secure coding is verified before release.

• Control change through change management and change control so every production change is authorised, tested, reviewed and reversible.

• Protect source code, build pipelines and release artefacts against tampering through version control, code review and code signing.

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 Secure development lifecycle

4.1.1 A secure development lifecycle shall be defined for all in-house and outsourced software development, with security requirements, threat modelling and security by design activities at each phase.

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

4.1.2 Developers shall follow the secure coding standard (OWASP ASVS-aligned): input validation, output encoding, parameterised queries, secure session handling and error handling that discloses nothing.

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.* Semi-annual. *Control owner.* Head of Compliance. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.1.3 Security testing shall be performed before release: static application security testing (SAST) on every build, software composition analysis for dependencies, dynamic testing (DAST) on staging and penetration testing for internet-facing or high-risk applications.

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

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

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

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

4.1.4 Development, test and production environments shall be segregated; production data shall not be used in development or test without masking and approval.

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

4.2 Source code, version control and code review

4.2.1 All source code and infrastructure-as-code shall be held in the enterprise version control system with branch protection, mandatory peer code review and an audit trail of every change.

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

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

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

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

4.2.2 Code review shall check security requirements and secure coding compliance; findings rated high or critical shall block the merge until resolved.

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

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

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

Test method. configuration review + sampling. *Frequency.* Semi-annual. *Control owner.* Head of Compliance. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2.3 Secrets shall never be committed to source code; secret scanning shall run on every commit and any exposed credential shall be rotated immediately.

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

4.2.4 Access to repositories shall be least-privilege and reviewed quarterly; committers shall be uniquely identified and commits to protected branches signed.

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.* Semi-annual. *Control owner.* Head of Compliance. *Status.* Implemented (self-declared by the document author; not independently verified).

4.3 Build pipeline, release and code signing

4.3.1 Builds shall run in a hardened, ephemeral pipeline; build artefacts shall be reproducible, code-signed and stored in a controlled artefact repository with integrity verification at deployment.

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

4.3.2 Third-party and open-source components shall be inventoried in a software bill of materials, assessed for known vulnerabilities and licence risk, and kept within supported versions.

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

4.3.3 Release to production shall require evidence of passed security testing, completed code review and an approved change record; releases shall be deployable by pipeline only, never by hand.

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

4.3.4 DevSecOps tooling results shall be tracked to closure and reported to the application security lead monthly.

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.* Semi-annual. *Control owner.* Head of Compliance. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.4 Change management and change control

4.4.1 All changes to production systems, applications, configurations and infrastructure shall be raised as change records, risk-assessed, tested and approved by the Change Advisory Board or, for pre-approved standard changes, by the change owner.

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

4.4.2 Emergency changes shall be authorised by the on-call change manager, implemented under supervision and reviewed retrospectively at the next Change Advisory Board.

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

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

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

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

4.4.3 Every change record shall include a rollback plan, a test result, the implementer and the approver; unauthorised changes shall be detected through configuration monitoring and treated as incidents.

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

4.4.4 Change success, failed-change and unauthorised-change rates shall be measured and reported monthly.

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

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is enforced at the identity provider and gateway with conditional access.

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

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

4.5 Application security in operation

4.5.1 Applications shall be maintained within vendor and community support; end-of-life frameworks and libraries shall be upgraded or removed within risk-based 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. automated telemetry review. *Frequency.* Semi-annual. *Control owner.* Head of Compliance. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5.2 Application security vulnerabilities reported by testing, bug bounty or vendors shall be triaged under the vulnerability management policy and remediated within 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. re-performance / observation. *Frequency.* Monthly. *Control owner.* Head of Compliance. *Status.* Implemented (self-declared by the document author; not independently verified).

4.5.3 Application logging shall record authentication, authorisation and data-access events sufficient for investigation, without logging secrets or personal information unnecessarily.

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

4.5.4 Application programming interfaces shall be authenticated, rate-limited, schema-validated and inventoried.

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

4.6 Outsourced and low-code development

4.6.1 Outsourced development shall be bound contractually to this standard, with rights to review code, test results and the supplier's secure development lifecycle evidence.

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

4.6.2 Low-code, scripting and robotic-process-automation artefacts that touch production data shall be held in version control and pass the same code review and change control as application code.

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

4.6.3 Acquired software shall be evaluated for secure development practices and known vulnerabilities before purchase.

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

4.7 Governance, accountability and policy lifecycle

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

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

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is enforced at the identity provider and gateway with conditional access.

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

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

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

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

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

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

Test method. automated telemetry review. *Frequency.* Monthly. *Control owner.* Head of Compliance. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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

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

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

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

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

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

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is implemented through the IGA/PAM platform with automated workflow and logging.

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

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

4.8 Risk assessment and treatment

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

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

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

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

Test method. configuration review + sampling. *Frequency.* Semi-annual. *Control owner.* Head of Compliance. *Status.* Partially implemented (self-declared by the document author; not independently verified).

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

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

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

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

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

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

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

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is implemented through the IGA/PAM platform with automated workflow and logging.

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

Test method. automated telemetry review. *Frequency.* Monthly. *Control owner.* Head of Compliance. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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

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

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

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

4.9 Monitoring, measurement and reporting

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

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

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

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

Test method. automated telemetry review. *Frequency.* Monthly. *Control owner.* Head of Compliance. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is implemented through the IGA/PAM platform with automated workflow and logging.

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

Test method. automated telemetry review. *Frequency.* Monthly. *Control owner.* Head of Compliance. *Status.* Partially implemented (self-declared by the document author; not independently verified).

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

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

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

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

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

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

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

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

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

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

4.10 Records, retention and evidence

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

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

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is implemented through the IGA/PAM platform with automated workflow and logging.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is monitored in the SIEM with detections mapped to the relevant threats.

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

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

4.11 Continuous improvement

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

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

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

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

Test method. automated telemetry review. *Frequency.* Semi-annual. *Control owner.* Head of Compliance. *Status.* Implemented (self-declared by the document author; not independently verified).

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

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

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

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

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

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

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

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is monitored in the SIEM with detections mapped to the relevant threats.

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

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

5. Roles and responsibilities (RACI)

Role	R	A	C	I	Responsibility
Head of Compliance	✓	✓			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 Product owner records security requirements and a threat model in the backlog before build starts.

6.2 Developer opens a pull request; the pipeline runs SAST, secret scanning and dependency checks; a peer performs code review and approves the merge.

6.3 Release manager raises the change record with test evidence and rollback plan; the Change Advisory Board approves; the pipeline deploys the signed artefact.

6.4 Application security lead reviews DevSecOps findings weekly and tracks high and critical findings to closure.

7. Monitoring, metrics and KPIs

Metric	Target	Frequency
Production changes with an approved change record	100%	Monthly
Pull requests merged with a completed code review	100%	Monthly
Critical or high SAST/SCA findings older than SLA	0	Monthly
Failed or backed-out changes	≤ 3%	Monthly
Unauthorised changes detected	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
Secure development lifecycle	The set of security activities integrated into each phase of software development.
Code review	Peer examination of a code change for correctness and security before it is merged.
Change control	The approval, testing and recording discipline applied to every production change.
Code signing	Cryptographically signing a build artefact so its origin and integrity can be verified at deployment.

11. Related documents

• Secure Software Development Standard

• Change & Release Management Procedure

• Change Management Policy

• Vulnerability 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: Build security into the software development lifecycle (SDLC) so applications are secure by design and secure coding is verified before release.

• Risk addressed: Control change through change management and change control so every production change is authorised, tested, reviewed and reversible.

• Risk addressed: Protect source code, build pipelines and release artefacts against tampering through version control, code review and code signing.

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	A secure development lifecycle shall be defined for all in-house and o…	ASD ISM	Monthly	Implemented
4.1.2	Developers shall follow the secure coding standard (OWASP ASVS-aligned…	Essential Eight	Semi-annual	Implemented
4.1.3	Security testing shall be performed before release: static application…	ISO/IEC 27001:2022	Semi-annual	Partially implemented
4.1.4	Development, test and production environments shall be segregated; pro…	SOC 2 (TSC)	Monthly	Implemented
4.2.1	All source code and infrastructure-as-code shall be held in the enterp…	APRA CPS 234	Semi-annual	Partially implemented
4.2.2	Code review shall check security requirements and secure coding compli…	ASD ISM	Annual	Implemented
4.2.3	Secrets shall never be committed to source code; secret scanning shall…	Essential Eight	Annual	Implemented
4.2.4	Access to repositories shall be least-privilege and reviewed quarterly…	ISO/IEC 27001:2022	Annual	Implemented
4.3.1	Builds shall run in a hardened, ephemeral pipeline; build artefacts sh…	SOC 2 (TSC)	Quarterly	Partially implemented
4.3.2	Third-party and open-source components shall be inventoried in a softw…	APRA CPS 234	Annual	Implemented
4.3.3	Release to production shall require evidence of passed security testin…	ASD ISM	Quarterly	Implemented
4.3.4	DevSecOps tooling results shall be tracked to closure and reported to …	Essential Eight	Annual	Implemented
4.4.1	All changes to production systems, applications, configurations and in…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.4.2	Emergency changes shall be authorised by the on-call change manager, i…	SOC 2 (TSC)	Semi-annual	Implemented
4.4.3	Every change record shall include a rollback plan, a test result, the …	APRA CPS 234	Monthly	Implemented
4.4.4	Change success, failed-change and unauthorised-change rates shall be m…	ASD ISM	Semi-annual	Implemented
4.5.1	Applications shall be maintained within vendor and community support; …	Essential Eight	Quarterly	Implemented
4.5.2	Application security vulnerabilities reported by testing, bug bounty o…	ISO/IEC 27001:2022	Monthly	Implemented
4.5.3	Application logging shall record authentication, authorisation and dat…	SOC 2 (TSC)	Annual	Implemented
4.5.4	Application programming interfaces shall be authenticated, rate-limite…	APRA CPS 234	Annual	Implemented
4.6.1	Outsourced development shall be bound contractually to this standard, …	ASD ISM	Monthly	Implemented
4.6.2	Low-code, scripting and robotic-process-automation artefacts that touc…	Essential Eight	Monthly	Implemented
4.6.3	Acquired software shall be evaluated for secure development practices …	ISO/IEC 27001:2022	Quarterly	Implemented

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

Appendix A — Control implementation checklist

Control area	Controls	Implementation status
Secure development lifecycle	4 control(s)	Implemented
Source code, version control and code review	4 control(s)	Implemented

Control area	Controls	Implementation status
Build pipeline, release and code signing	4 control(s)	Partially implemented
Change management and change control	4 control(s)	Planned
Application security in operation	4 control(s)	Partially implemented
Outsourced and low-code development	3 control(s)	Implemented
Governance, accountability and policy lifecycle	4 control(s)	Implemented
Risk assessment and treatment	4 control(s)	Implemented
Monitoring, measurement and reporting	4 control(s)	Planned
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
Secure development lifecycle	4	Configuration review + sampling	Config export + screenshots	Semi-annual
Source code, version control and code review	4	Automated control telemetry	Dashboard / telemetry extract	Quarterly
Build pipeline, release and code signing	4	Evidence inspection + interview	Approved records + tickets	Monthly
Change management and change control	4	Re-performance / observation	Observed run + sign-off	Annual
Application security in operation	4	Log and exception review	SIEM / log extract	Monthly
Outsourced and low-code development	3	Independent test / scan	Scan / test report	Monthly
Governance, accountability and policy lifecycle	4	Configuration review + sampling	Config export + screenshots	Annual
Risk assessment and treatment	4	Automated control telemetry	Dashboard / telemetry extract	Annual
Monitoring, measurement and reporting	4	Evidence inspection + interview	Approved records + tickets	Monthly
Records, retention and evidence	4	Re-performance / observation	Observed run + sign-off	Annual
Continuous improvement	3	Log and exception review	SIEM / log extract	Quarterly

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

13. Document approval and distribution

Approval	Name	Role	Date
Prepared by	David Okafor	Head of Compliance	10 Oct 2026
Reviewed by	Laura Mendez	Third-Party Risk 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

Abbreviation	Meaning
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	Tom Bauer	Initial issue.
2.0	02 Oct 2024	Aisha Khan	Annual review; control uplift and framework alignment.
3.3	02 Oct 2025	David Okafor	Updated for current framework versions and cloud scope.