Southern Mutual Bank

51 824 753 556

Personnel Security Screening, Onboarding & Offboarding Procedure

Procedure · synthetic assessor-grade test document

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

Document ID	SOU-PRO-0043
Version	2.3
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 personnel security screening, onboarding & offboarding 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, ISO/IEC 27001:2022, APRA CPS 234, APRA CPS 230. It applies to Core banking platform and supporting services.

Control objectives:

• Prevent unauthorised physical access to facilities, secure areas, equipment and media through layered physical security and physical protection controls.

• Ensure personnel security: pre-employment personnel screening, background checks and security clearances proportionate to role, and controlled termination of employment.

• Sustain security awareness and awareness training so staff recognise and report insider threat, tailgating and social-engineering attempts.

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, ISO/IEC 27001:2022, APRA CPS 234, APRA CPS 230. Where an obligation is more stringent in one framework, the most stringent requirement applies.

4. Requirements

4.1 Physical access control and secure areas

4.1.1 Physical access to data centres, communications rooms and other secure areas shall be restricted to authorised personnel using access cards, PIN and, for the highest-security rooms, biometric physical access control.

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 Physical access rights shall be granted on a need-to-enter basis by the facility owner, recorded in the physical access register, and reviewed at least quarterly; access for leavers shall be revoked on the day of termination of employment.

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

4.1.3 Visitors and contractors shall be pre-registered, identity-checked at reception, issued a visible temporary pass, escorted at all times in secure areas and signed out on departure; the visitor log shall be retained for 12 months.

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).

4.1.4 Tailgating and piggybacking shall be prevented by anti-passback turnstiles or mantraps at secure-area entrances, and every attempt shall be reported as a physical security event.

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).

4.2 Physical and environmental protection of equipment

4.2.1 Physical and environmental controls shall protect equipment against fire, flood, power failure and temperature or humidity excursions: fire detection and suppression, dual power feeds with UPS and generator, and

environmental monitoring with alerting.

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

4.2.2 CCTV shall cover all entrances to secure areas and the interior of data-centre halls; footage shall be retained for at least 90 days and reviewed on any physical security event.

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

4.2.3 Equipment, media and paper records shall be protected against theft and unauthorised viewing through a clear-desk and clear-screen rule, locked storage for classified material and secure cabling routes.

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 Equipment taken off-site shall be authorised, recorded and protected in transit; equipment and media shall be sanitised before reuse or disposal.

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

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

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

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

4.3 Personnel screening and clearances

4.3.1 Personnel screening shall be completed before access is granted: identity verification, right-to-work, qualification and employment-history checks, and a national police background check; roles with privileged or high-risk access shall require enhanced background checks and, where mandated, an Australian Government security clearance.

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

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

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

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

4.3.2 Security clearances and screening outcomes shall be recorded in the personnel security register, re-validated at defined intervals and on change of role, and revoked on termination of employment.

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

4.3.3 Contractors and third-party staff shall be screened to the same standard as employees for the access they hold, and their sponsors shall confirm continued need at least annually.

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

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

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

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

4.3.4 Adverse screening findings shall be risk-assessed by People & Culture and Security before an offer is confirmed, and the decision recorded.

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 Terms of employment, conduct and termination

4.4.1 Employment contracts and contractor agreements shall include confidentiality, acceptable-use and security responsibilities that survive termination of employment.

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

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is aligned to the CIS-equivalent secure baseline and enforced via platform policy.

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

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

4.4.2 Breaches of security obligations shall be handled through the disciplinary process, proportionate to the breach and consistently applied.

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

4.4.3 On termination of employment or change of role, access cards, tokens, keys, devices and information shall be returned and logical and physical access revoked within one business day, immediately for involuntary

departures.

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 Exit interviews shall remind departing personnel of their continuing confidentiality obligations and record the return of assets.

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

4.5 Physical connections to managed interfaces

4.5.1 Unauthorised physical connections at managed network interfaces shall be prevented: unused switch ports shut down, 802.1X port-based network access control on user-facing ports, and patch panels, network devices and cabling housed in locked racks within secure areas.

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).

4.5.2 Physical access to communications rooms and network device consoles shall be logged and reviewed; CCTV shall cover rack rows.

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

4.5.3 Devices found connected without authorisation shall be reported as a physical security event and isolated pending investigation.

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

4.6 Security awareness, training and insider threat

4.6.1 All personnel shall complete security awareness training at onboarding and at least annually; completion shall be tracked and non-completion escalated to people leaders.

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

4.6.2 Role-based security training shall be provided to privileged users, developers, incident responders and personnel handling classified or personal information.

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

4.6.3 An insider threat programme shall combine personnel security, monitoring of privileged activity and a confidential reporting channel; indicators shall be triaged by Security and People & Culture.

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

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

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

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

4.6.4 Awareness and training effectiveness shall be measured through phishing simulation results, assessment scores and reported-incident trends.

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

4.7 Secure area operations and supporting utilities

4.7.1 Secure areas shall have documented operating rules: no unaccompanied visitors, no photography, no removable media without authorisation, and periodic physical security inspections recorded by the facility 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.* Monthly. *Control owner.* Head of Compliance. *Status.* Implemented (self-declared by the document author; not independently verified).

4.7.2 Supporting utilities (power, cooling, water, telecommunications) shall have redundancy proportionate to the criticality of the equipment they serve and shall be tested on a defined schedule.

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

4.7.3 Delivery and loading areas shall be isolated from secure areas, and incoming equipment inspected before being brought into the data centre.

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

4.8 Governance, accountability and policy lifecycle

4.8.1 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 supports timely detection, response and recovery and meets regulatory obligations.

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

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

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

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

4.8.3 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 enforces least privilege, accountability and limits the blast radius of compromise.

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

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

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

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

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

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

hardening standard with drift monitoring and alerting.

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

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

4.9 Risk assessment and treatment

4.9.1 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 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).

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

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).

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

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

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

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

4.10 Monitoring, measurement and reporting

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

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

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

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

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

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

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 Records, retention and evidence

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

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

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

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

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

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

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

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

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

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

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 aligned to the CIS-equivalent secure baseline and enforced via platform policy.

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

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

4.12 Continuous improvement

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

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

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

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

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

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

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

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

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

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

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

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 aligned to the CIS-equivalent secure baseline and enforced via platform policy.

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

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

5. Roles and responsibilities (RACI)

Role	R	A	C	I	Responsibility
Head of 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 Facility owner approves physical access requests in the ITSM tool; Security issues the access card and records the grant in the physical access register.

6.2 Reception verifies visitor identity, issues a temporary pass and records arrival and departure in the visitor log; the host escorts the visitor throughout.

6.3 People & Culture completes personnel screening and background checks before start date and records outcomes in the personnel security register.

6.4 On a leaver notification, People & Culture triggers the termination of employment checklist: asset return, access-card deactivation, account revocation, exit interview.

6.5 Learning platform assigns security awareness training annually and reports completion; Security runs quarterly phishing simulation and reports results.

7. Monitoring, metrics and KPIs

Metric	Target	Frequency
Physical access rights reviewed on schedule	100%	Quarterly
Leaver access cards deactivated within 1 business day	≥ 99%	Monthly
Personnel screening completed before start date	100%	Monthly
Security awareness training completion	≥ 98%	Quarterly
Physical security events investigated within 5 days	100%	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 area	A room or zone whose physical access is restricted to authorised personnel and monitored.
Personnel screening	Pre-employment and periodic identity, background and clearance checks proportionate to role.
Security clearance	A formal authorisation to access classified information, granted after vetting.

Term	Definition
Insider threat	The risk that a person with authorised access misuses it, deliberately or negligently.

11. Related documents

• Physical & Environmental Security Policy

• Personnel Security Screening, Onboarding & Offboarding Procedure

• Security Awareness & Training Policy

• Acceptable Use Policy

12. Control framework mapping

Framework	Indicative mapped controls
ASD ISM	Guidelines: Access, System hardening, Monitoring
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23
APRA CPS 234	Information security capability, Control testing, Incident notification
APRA CPS 230	Critical operations, Tolerance levels, Service provider management

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: Prevent unauthorised physical access to facilities, secure areas, equipment and media through layered physical security and physical protection controls.

• Risk addressed: Ensure personnel security: pre-employment personnel screening, background checks and security clearances proportionate to role, and controlled termination of employment.

• Risk addressed: Sustain security awareness and awareness training so staff recognise and report insider threat, tailgating and social-engineering attempts.

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	Physical access to data centres, communications rooms and other secure…	ASD ISM	Quarterly	Implemented
4.1.2	Physical access rights shall be granted on a need-to-enter basis by th…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.1.3	Visitors and contractors shall be pre-registered, identity-checked at …	APRA CPS 234	Annual	Implemented
4.1.4	Tailgating and piggybacking shall be prevented by anti-passback turnst…	APRA CPS 230	Semi-annual	Implemented
4.2.1	Physical and environmental controls shall protect equipment against fi…	ASD ISM	Monthly	Implemented
4.2.2	CCTV shall cover all entrances to secure areas and the interior of dat…	ISO/IEC 27001:2022	Annual	Implemented
4.2.3	Equipment, media and paper records shall be protected against theft an…	APRA CPS 234	Quarterly	Implemented
4.2.4	Equipment taken off-site shall be authorised, recorded and protected i…	APRA CPS 230	Semi-annual	Partially implemented
4.3.1	Personnel screening shall be completed before access is granted: ident…	ASD ISM	Quarterly	Implemented
4.3.2	Security clearances and screening outcomes shall be recorded in the pe…	ISO/IEC 27001:2022	Monthly	Implemented
4.3.3	Contractors and third-party staff shall be screened to the same standa…	APRA CPS 234	Annual	Implemented
4.3.4	Adverse screening findings shall be risk-assessed by People & Culture …	APRA CPS 230	Semi-annual	Implemented
4.4.1	Employment contracts and contractor agreements shall include confident…	ASD ISM	Semi-annual	Implemented
4.4.2	Breaches of security obligations shall be handled through the discipli…	ISO/IEC 27001:2022	Monthly	Implemented
4.4.3	On termination of employment or change of role, access cards, tokens, …	APRA CPS 234	Semi-annual	Implemented
4.4.4	Exit interviews shall remind departing personnel of their continuing c…	APRA CPS 230	Annual	Implemented
4.5.1	Unauthorised physical connections at managed network interfaces shall …	ASD ISM	Monthly	Implemented
4.5.2	Physical access to communications rooms and network device consoles sh…	ISO/IEC 27001:2022	Monthly	Implemented
4.5.3	Devices found connected without authorisation shall be reported as a p…	APRA CPS 234	Monthly	Partially implemented
4.6.1	All personnel shall complete security awareness training at onboarding…	APRA CPS 230	Monthly	Implemented
4.6.2	Role-based security training shall be provided to privileged users, de…	ASD ISM	Semi-annual	Implemented
4.6.3	An insider threat programme shall combine personnel security, monitori…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.6.4	Awareness and training effectiveness shall be measured through phishin…	APRA CPS 234	Monthly	Partially implemented
4.7.1	Secure areas shall have documented operating rules: no unaccompanied v…	APRA CPS 230	Semi-annual	Implemented

Ref	Control statement	Framework	Test freq.	Status
4.7.2	Supporting utilities (power, cooling, water, telecommunications) shall…	ASD ISM	Quarterly	Implemented
4.7.3	Delivery and loading areas shall be isolated from secure areas, and in…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.8.1	A named executive owner shall be accountable for this control area and…	APRA CPS 234	Annual	Partially implemented
4.8.2	This document shall be reviewed at least annually and after any materi…	APRA CPS 230	Quarterly	Implemented
4.8.3	Roles and responsibilities shall align to the three-lines-of-defence m…	ASD ISM	Annual	Implemented
4.8.4	Material decisions, approvals and deviations shall be minuted and reta…	ISO/IEC 27001:2022	Quarterly	Partially implemented
4.9.1	Risks within this control area shall be identified, assessed (likeliho…	APRA CPS 234	Semi-annual	Implemented
4.9.2	Residual risk exceeding the approved risk appetite shall be escalated …	APRA CPS 230	Semi-annual	Implemented
4.9.3	Risk assessments shall be refreshed on a defined cadence and upon sign…	ASD ISM	Monthly	Partially implemented
4.9.4	Key risk indicators (KRIs) shall be defined and monitored against thre…	ISO/IEC 27001:2022	Monthly	Implemented
4.10.1	Control performance shall be monitored continuously through automated …	APRA CPS 234	Monthly	Implemented
4.10.2	The metrics and targets in this document shall be reported monthly to …	APRA CPS 230	Monthly	Partially implemented
4.10.3	Control failures and exceptions shall be logged, triaged by severity a…	ASD ISM	Annual	Partially implemented
4.10.4	Independent assurance (internal audit / external assessment) shall per…	ISO/IEC 27001:2022	Annual	Implemented
4.11.1	Evidence demonstrating the operation of these controls shall be genera…	APRA CPS 234	Semi-annual	Implemented
4.11.2	Evidence shall be sufficient for an independent assessor to conclude o…	APRA CPS 230	Monthly	Implemented
4.11.3	Access to control evidence shall be least-privilege and itself logged;…	ASD ISM	Annual	Implemented
4.11.4	On decommissioning, records shall be retained or disposed of per the r…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.12.1	Lessons from incidents, audits, assessments and exercises shall be fed…	APRA CPS 234	Semi-annual	Implemented
4.12.2	Control maturity shall be assessed against a defined target state, wit…	APRA CPS 230	Quarterly	Implemented
4.12.3	Automation and tooling shall be progressively adopted to reduce manual…	ASD ISM	Annual	Partially implemented

Appendix A — Control implementation checklist

Control area	Controls	Implementation status
Physical access control and secure areas	4 control(s)	Planned

Control area	Controls	Implementation status
Physical and environmental protection of equipment	4 control(s)	Implemented
Personnel screening and clearances	4 control(s)	Implemented
Terms of employment, conduct and termination	4 control(s)	Implemented
Physical connections to managed interfaces	3 control(s)	Partially implemented
Security awareness, training and insider threat	4 control(s)	Planned
Secure area operations and supporting utilities	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)	Planned
Continuous improvement	3 control(s)	Planned

Appendix B — Control testing and evidence matrix

Control area	Ctrls	Test method	Evidence	Frequency
Physical access control and secure areas	4	Configuration review + sampling	Config export + screenshots	Monthly
Physical and environmental protection of equipment	4	Automated control telemetry	Dashboard / telemetry extract	Quarterly
Personnel screening and clearances	4	Evidence inspection + interview	Approved records + tickets	Quarterly
Terms of employment, conduct and termination	4	Re-performance / observation	Observed run + sign-off	Monthly
Physical connections to managed interfaces	3	Log and exception review	SIEM / log extract	Semi-annual
Security awareness, training and insider threat	4	Independent test / scan	Scan / test report	Quarterly
Secure area operations and supporting utilities	3	Configuration review + sampling	Config export + screenshots	Semi-annual
Governance, accountability and policy lifecycle	4	Automated control telemetry	Dashboard / telemetry extract	Monthly
Risk assessment and treatment	4	Evidence inspection + interview	Approved records + tickets	Semi-annual
Monitoring, measurement and reporting	4	Re-performance / observation	Observed run + sign-off	Semi-annual
Records, retention and evidence	4	Log and exception review	SIEM / log extract	Quarterly
Continuous improvement	3	Independent test / scan	Scan / test report	Quarterly

Evidence is retained for audit per the records-retention schedule and crosswalked to ASD ISM, ISO/IEC 27001:2022, APRA CPS 234, APRA CPS 230.

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

15. Revision history

Version	Date	Author	Summary of change
1.0	03 Oct 2024	Tom Bauer	Initial issue.
2.3	02 Oct 2025	Aisha Khan	Annual review; control uplift and framework alignment.