Southern Mutual Bank

51 824 753 556

Access Control Policy

Policy · synthetic assessor-grade test document

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

Document ID	SOU-POL-0002
Version	3.2
Owner	James O'Connor (Head of Operational Risk)
Approved by	CISO
Classification	Internal Use Only
Status	Approved — In force
Effective date	14 Mar 2026
Next review	14 Mar 2027

1. Purpose and control objectives

This policy establishes the requirements, accountabilities and control objectives for access control policy 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:

• Ensure access to information and systems is granted, reviewed and revoked on a least-privilege, need-to-know basis.

• Prevent unauthorised access through strong authentication, segregation of duties and privileged-access control.

• Provide an auditable trail of who has access to what, why, and when it was last confirmed.

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 Access provisioning and authorisation

4.1.1 Access shall be requested through the IT Service Management workflow and authorised by the relevant system owner before provisioning; verbal or email-only approvals are not accepted.

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

Implementation. Responsibility, frequency and the system(s) of record are defined; results are reported to the control owner and second-line risk, and tracked to closure where below target. The control is configured per the hardening standard with drift monitoring and alerting.

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

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

4.1.2 Role-based access profiles shall be defined per system and mapped to job functions; ad-hoc grants outside an approved role require documented risk acceptance.

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

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

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

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

4.1.3 Joiner, mover and leaver (JML) events shall trigger automated provisioning and de-provisioning workflows integrated with the HR system of record.

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

4.1.4 Birthright access shall be limited to the minimum required for a role; all elevated entitlements are request-and-approve.

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

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

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

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

4.2 Authentication and credentials

4.2.1 Multi-factor authentication (MFA) shall be enforced for all remote, administrative, internet-facing and customer access, using phishing-resistant factors where supported.

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

4.2.2 Passwords shall meet the enterprise credential standard (length, complexity, screening against breached-password lists) and never be shared or reused across accounts.

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

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

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

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

4.2.3 Service and application accounts shall have credentials vaulted in the Privileged Access Management (PAM) platform, rotated automatically, and excluded from interactive logon.

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

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

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

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

4.2.4 Single sign-on (SSO) via the enterprise identity provider shall be the default; local accounts are permitted only where SSO is technically infeasible and are compensated.

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

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

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

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

4.3 Privileged access management

4.3.1 Privileged access shall be brokered through the PAM platform with just-in-time elevation, session recording and automatic credential check-in.

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

4.3.2 Standing privileged access shall be eliminated wherever feasible; break-glass accounts shall be vaulted, alerted on use, and reviewed after every invocation.

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

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

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

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

4.3.3 Administrative actions shall be performed from hardened privileged access workstations on a segmented management network.

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

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

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

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

4.3.4 Privileged entitlements shall be recertified at least quarterly with evidence retained for audit.

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

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

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

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

4.4 Segregation of duties

4.4.1 Segregation of duties (SoD) shall be enforced so that no single individual can initiate and approve a high-risk transaction, change or access grant.

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

4.4.2 SoD conflict rules shall be defined, encoded in the access-governance tooling, and tested at provisioning and recertification.

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

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

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

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

4.4.3 Where an SoD conflict cannot be removed, a documented compensating control and risk acceptance shall be recorded and monitored.

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

4.5 Access review and recertification

4.5.1 User access rights shall be recertified at least quarterly for privileged accounts and semi-annually for standard accounts.

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

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

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

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

4.5.2 Recertification campaigns shall require an explicit approve/revoke decision by the accountable manager; non-response defaults to revocation.

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

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

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

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

4.5.3 Access for terminated personnel shall be revoked within one business day, and immediately for involuntary terminations.

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

4.5.4 Dormant accounts (no logon within 45 days) shall be flagged, suspended, and removed per 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. re-performance / observation. *Frequency.* Annual. *Control owner.* Head of Operational Risk. *Status.* Implemented (self-declared by the document author; not independently verified).

4.6 Remote and third-party access

4.6.1 Remote access shall require MFA and a managed or compliant device, terminating into a controlled, monitored zone.

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

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

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

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

4.6.2 Third-party and vendor access shall be time-bound, sponsored by a named owner, brokered through the PAM platform and revoked on engagement end.

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

4.6.3 Just-in-time access shall be used for elevated and emergency scenarios, with automatic expiry and post-use review.

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

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

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

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

4.6.4 Access from unmanaged or unknown locations/devices shall be blocked or step-up authenticated per the conditional-access policy.

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

4.7 Customer authentication and account protection

4.7.1 Customer authentication shall use strong, phishing-resistant methods for high-risk actions (payments, payee changes, profile updates).

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

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

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

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

4.7.2 Step-up authentication and transaction signing shall be enforced for high-value or anomalous transactions.

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

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

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

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

4.7.3 Account-takeover controls (device binding, velocity checks, impossible-travel detection) shall be implemented and monitored.

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

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

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

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

4.7.4 Customer credential resets shall follow an identity-proofing standard proportionate to risk.

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

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

5. Roles and responsibilities (RACI)

Role	R	A	C	I	Responsibility
Head of Operational Risk	✓	✓			Owns this document; ensures it is current, resourced and effective.
System / Asset owners	✓		✓		Implement and operate the controls in their scope.
Security Operations	✓		✓	✓	Monitors compliance; investigates and responds to exceptions.
Risk & Compliance (2nd line)			✓	✓	Provides oversight, challenge and reporting.
Internal Audit (3rd line)				✓	Independent assurance over design and operating effectiveness.

Role	R	A	C	I	Responsibility
All staff & contractors	✓			✓	Comply with the requirements; report suspected breaches.

6. Procedures and implementation

6.1 Raise an access request in the ITSM tool selecting the target system, role profile and business justification.

6.2 System owner reviews and approves/declines; PAM/IGA tooling provisions the entitlement on approval.

6.3 Quarterly the IGA platform launches recertification campaigns to accountable managers.

6.4 SOC monitors privileged sessions and alerts on break-glass use and anomalous access.

7. Monitoring, metrics and KPIs

Metric	Target	Frequency
Privileged accounts recertified on time	100%	Quarterly
Leaver access revoked within 1 business day	≥ 99%	Monthly
MFA coverage of eligible accounts	100%	Monthly
Open SoD conflicts without risk acceptance	0	Monthly
Dormant accounts older than 45 days	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
Privileged access	Access permitting administrative or security-relevant control of a system.
Break-glass account	A vaulted emergency account used only under controlled, alerted conditions.
Recertification	Periodic manager attestation that an individual still requires their access.
Segregation of duties	A control ensuring no one person can complete a high-risk action unchecked.

11. Related documents

- Information Security Policy
- Privileged Access Management Standard
- Identity & Access Management Standard
- Multi-Factor Authentication Standard

12. Control framework mapping

Framework	Indicative mapped controls
ASD ISM	Guidelines: Access, System hardening, Monitoring

Framework	Indicative mapped controls
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: Ensure access to information and systems is granted, reviewed and revoked on a least-privilege, need-to-know basis.

• Risk addressed: Prevent unauthorised access through strong authentication, segregation of duties and privileged-access control.

• Risk addressed: Provide an auditable trail of who has access to what, why, and when it was last confirmed.

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	Access shall be requested through the IT Service Management workflow a…	ASD ISM	Quarterly	Implemented
4.1.2	Role-based access profiles shall be defined per system and mapped to j…	Essential Eight	Quarterly	Implemented
4.1.3	Joiner, mover and leaver (JML) events shall trigger automated provisio…	ISO/IEC 27001:2022	Monthly	Implemented
4.1.4	Birthright access shall be limited to the minimum required for a role;…	SOC 2 (TSC)	Quarterly	Implemented
4.2.1	Multi-factor authentication (MFA) shall be enforced for all remote, ad…	APRA CPS 234	Quarterly	Implemented
4.2.2	Passwords shall meet the enterprise credential standard (length, compl…	ASD ISM	Annual	Partially implemented
4.2.3	Service and application accounts shall have credentials vaulted in the…	Essential Eight	Monthly	Implemented

Ref	Control statement	Framework	Test freq.	Status
4.2.4	Single sign-on (SSO) via the enterprise identity provider shall be the…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.3.1	Privileged access shall be brokered through the PAM platform with just…	SOC 2 (TSC)	Annual	Partially implemented
4.3.2	Standing privileged access shall be eliminated wherever feasible; brea…	APRA CPS 234	Annual	Implemented
4.3.3	Administrative actions shall be performed from hardened privileged acc…	ASD ISM	Monthly	Implemented
4.3.4	Privileged entitlements shall be recertified at least quarterly with e…	Essential Eight	Annual	Implemented
4.4.1	Segregation of duties (SoD) shall be enforced so that no single indivi…	ISO/IEC 27001:2022	Quarterly	Implemented
4.4.2	SoD conflict rules shall be defined, encoded in the access-governance …	SOC 2 (TSC)	Semi-annual	Partially implemented
4.4.3	Where an SoD conflict cannot be removed, a documented compensating con…	APRA CPS 234	Monthly	Implemented
4.5.1	User access rights shall be recertified at least quarterly for privile…	ASD ISM	Semi-annual	Implemented
4.5.2	Recertification campaigns shall require an explicit approve/revoke dec…	Essential Eight	Semi-annual	Implemented
4.5.3	Access for terminated personnel shall be revoked within one business d…	ISO/IEC 27001:2022	Quarterly	Implemented
4.5.4	Dormant accounts (no logon within 45 days) shall be flagged, suspended…	SOC 2 (TSC)	Semi-annual	Implemented
4.6.1	Remote access shall require MFA and a managed or compliant device, ter…	APRA CPS 234	Annual	Partially implemented
4.6.2	Third-party and vendor access shall be time-bound, sponsored by a name…	ASD ISM	Monthly	Implemented
4.6.3	Just-in-time access shall be used for elevated and emergency scenarios…	Essential Eight	Annual	Implemented
4.6.4	Access from unmanaged or unknown locations/devices shall be blocked or…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.7.1	Customer authentication shall use strong, phishing-resistant methods f…	SOC 2 (TSC)	Annual	Partially implemented
4.7.2	Step-up authentication and transaction signing shall be enforced for h…	APRA CPS 234	Quarterly	Implemented
4.7.3	Account-takeover controls (device binding, velocity checks, impossible…	ASD ISM	Monthly	Implemented
4.7.4	Customer credential resets shall follow an identity-proofing standard …	Essential Eight	Quarterly	Implemented
4.8.1	A named executive owner shall be accountable for this control area and…	ISO/IEC 27001:2022	Semi-annual	Implemented
4.8.2	This document shall be reviewed at least annually and after any materi…	SOC 2 (TSC)	Monthly	Implemented
4.8.3	Roles and responsibilities shall align to the three-lines-of-defence m…	APRA CPS 234	Monthly	Implemented
4.8.4	Material decisions, approvals and deviations shall be minuted and reta…	ASD ISM	Quarterly	Implemented

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

Appendix A — Control implementation checklist

Control area	Controls	Implementation status
Access provisioning and authorisation	4 control(s)	Planned
Authentication and credentials	4 control(s)	Implemented
Privileged access management	4 control(s)	Implemented
Segregation of duties	3 control(s)	Implemented
Access review and recertification	4 control(s)	Implemented
Remote and third-party access	4 control(s)	Planned
Customer authentication and account protection	4 control(s)	Implemented
Governance, accountability and policy lifecycle	4 control(s)	Partially implemented
Risk assessment and treatment	4 control(s)	Implemented
Monitoring, measurement and reporting	4 control(s)	Implemented
Records, retention and evidence	4 control(s)	Implemented

Control area	Controls	Implementation status
Continuous improvement	3 control(s)	Planned

Appendix B — Control testing and evidence matrix

Control area	Ctrls	Test method	Evidence	Frequency
Access provisioning and authorisation	4	Configuration review + sampling	Config export + screenshots	Monthly
Authentication and credentials	4	Automated control telemetry	Dashboard / telemetry extract	Annual
Privileged access management	4	Evidence inspection + interview	Approved records + tickets	Semi-annual
Segregation of duties	3	Re-performance / observation	Observed run + sign-off	Semi-annual
Access review and recertification	4	Log and exception review	SIEM / log extract	Monthly
Remote and third-party access	4	Independent test / scan	Scan / test report	Annual
Customer authentication and account protection	4	Configuration review + sampling	Config export + screenshots	Monthly
Governance, accountability and policy lifecycle	4	Automated control telemetry	Dashboard / telemetry extract	Quarterly
Risk assessment and treatment	4	Evidence inspection + interview	Approved records + tickets	Annual
Monitoring, measurement and reporting	4	Re-performance / observation	Observed run + sign-off	Quarterly
Records, retention and evidence	4	Log and exception review	SIEM / log extract	Semi-annual
Continuous improvement	3	Independent test / scan	Scan / test report	Annual

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

13. Document approval and distribution

Approval	Name	Role	Date
Prepared by	James O'Connor	Head of Operational Risk	10 Oct 2026
Reviewed by	Aisha Khan	Security Operations Lead	20 Oct 2026
Approved by	Priya Sharma	Chief Information Security Officer	26 Oct 2026
Endorsed by	—	Board Risk Committee	30 Oct 2026

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

14. Abbreviations

Abbreviation	Meaning
ISMS	Information Security Management System
MFA / SSO	Multi-Factor Authentication / Single Sign-On
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	David Okafor	Initial issue.
2.0	02 Oct 2024	Tom Bauer	Annual review; control uplift and framework alignment.
3.2	02 Oct 2025	James O'Connor	Updated for current framework versions and cloud scope.