Southern Mutual Bank

51 824 753 556

Third-Party Risk Management Policy

Policy · synthetic assessor-grade test document

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

Document ID	SOU-POL-0019
Version	2.4
Owner	Greg Thompson (Network Security Lead)
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 third-party risk management policy across Southern Mutual Bank (“the Bank”). It forms part of the Bank's Information Security Management System and supports its obligations under TPRM, APRA CPS 230, ISO/IEC 27001:2022. It applies to Core banking platform and supporting services.

Control objectives:

• Ensure third parties and material service providers meet the organisation's security and resilience obligations.

• Manage concentration, chain-supplier and exit risk for critical dependencies.

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

4. Requirements

4.1 Onboarding and due diligence

4.1.1 Material service providers shall be risk-assessed before engagement and re-assessed at least annually.

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.* Annual. *Control owner.* Network Security Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.1.2 Security obligations, right-to-audit, breach-notification and sub-contracting clauses shall be included in material supplier contracts.

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

4.1.3 Supplier assurance evidence (e.g. SOC 2 Type II, ISO 27001) shall be obtained and reviewed; gaps tracked to closure.

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.* Annual. *Control owner.* Network Security Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2 Ongoing monitoring

4.2.1 Supplier performance and control posture shall be monitored against the contract and SLAs.

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.* Semi-annual. *Control owner.* Network Security Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.2.2 The shared-responsibility matrix and inherited controls shall be documented and kept current.

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.* Monthly. *Control owner.* Network Security Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.2.3 Material incidents at suppliers shall be notified to the organisation and assessed for impact.

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.* Monthly. *Control owner.* Network Security Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.3 Concentration and exit

4.3.1 Concentration and chain-supplier risk shall be assessed and reported to the risk committee.

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

4.3.2 Exit plans shall be maintained and tested for material service providers supporting critical operations.

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

4.3.3 Stressed-exit scenarios shall consider data return/destruction, continuity and substitutability.

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

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

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

Test method. automated telemetry review. *Frequency.* Semi-annual. *Control owner.* Network Security Lead. *Status.* Partially implemented (self-declared by the document author; not independently verified).

4.4 Cloud and SaaS provider governance

4.4.1 Cloud and SaaS providers shall be assessed for security, resilience and data-handling before adoption and periodically thereafter.

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

4.4.2 The shared-responsibility model shall be documented per provider and inherited controls evidenced.

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.* Semi-annual. *Control owner.* Network Security Lead. *Status.* Implemented (self-declared by the document author; not independently verified).

4.4.3 SaaS sprawl shall be discovered and brought under management; unsanctioned SaaS shall be remediated.

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

4.4.4 Provider security posture (certifications, incidents, breach notifications) shall be monitored.

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

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

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

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

4.5 Fourth-party and concentration risk

4.5.1 Material sub-contractors (fourth parties) shall be identified and assessed for chain-supplier risk.

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

4.5.2 Concentration risk across critical providers shall be assessed and reported to the risk committee.

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

4.5.3 Stressed-exit and substitutability shall be considered for concentrated dependencies.

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

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

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

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

4.5.4 Contractual flow-down of security and notification obligations to sub-contractors shall be required.

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

4.6 Governance, accountability and policy lifecycle

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.7 Risk assessment and treatment

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.8 Monitoring, measurement and reporting

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.9 Records, retention and evidence

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.10 Continuous improvement

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. Roles and responsibilities (RACI)

Role	R	A	C	I	Responsibility
Network Security Lead	✓	✓			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 Procurement triggers a risk assessment; TPRM classifies materiality and required assurance.

6.2 Assurance evidence is collected and reviewed at onboarding and annually.

6.3 Exit plans are documented for material providers and tested per schedule.

7. Monitoring, metrics and KPIs

Metric	Target	Frequency
Material suppliers risk-assessed in date	100%	Quarterly
Material suppliers with current assurance evidence	≥ 95%	Quarterly
Material suppliers with tested exit plan	100%	Annual
Overdue supplier remediation actions	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
Material service provider	A provider whose failure would materially affect a critical operation.
Shared-responsibility matrix	Mapping of which controls the provider operates vs the customer.
Stressed exit	Unplanned termination of a provider while maintaining critical operations.

11. Related documents

• Third-Party Risk Management Policy

• Vendor Security Assessment Standard

• Operational Resilience Policy (CPS 230)

12. Control framework mapping

Framework	Indicative mapped controls
TPRM	Due diligence, Ongoing monitoring
APRA CPS 230	Critical operations, Tolerance levels, Service provider management
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23

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 third parties and material service providers meet the organisation's security and resilience obligations.

• Risk addressed: Manage concentration, chain-supplier and exit risk for critical dependencies.

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	Material service providers shall be risk-assessed before engagement an…	TPRM	Quarterly	Partially implemented
4.1.2	Security obligations, right-to-audit, breach-notification and sub-cont…	APRA CPS 230	Semi-annual	Implemented
4.1.3	Supplier assurance evidence (e.g. SOC 2 Type II, ISO 27001) shall be o…	ISO/IEC 27001:2022	Quarterly	Partially implemented
4.2.1	Supplier performance and control posture shall be monitored against th…	TPRM	Semi-annual	Implemented
4.2.2	The shared-responsibility matrix and inherited controls shall be docum…	APRA CPS 230	Quarterly	Partially implemented
4.2.3	Material incidents at suppliers shall be notified to the organisation …	ISO/IEC 27001:2022	Semi-annual	Implemented
4.3.1	Concentration and chain-supplier risk shall be assessed and reported t…	TPRM	Annual	Partially implemented
4.3.2	Exit plans shall be maintained and tested for material service provide…	APRA CPS 230	Monthly	Implemented
4.3.3	Stressed-exit scenarios shall consider data return/destruction, contin…	ISO/IEC 27001:2022	Monthly	Implemented
4.4.1	Cloud and SaaS providers shall be assessed for security, resilience an…	TPRM	Monthly	Implemented
4.4.2	The shared-responsibility model shall be documented per provider and i…	APRA CPS 230	Annual	Implemented
4.4.3	SaaS sprawl shall be discovered and brought under management; unsancti…	ISO/IEC 27001:2022	Quarterly	Implemented
4.4.4	Provider security posture (certifications, incidents, breach notificat…	TPRM	Monthly	Implemented
4.5.1	Material sub-contractors (fourth parties) shall be identified and asse…	APRA CPS 230	Quarterly	Implemented
4.5.2	Concentration risk across critical providers shall be assessed and rep…	ISO/IEC 27001:2022	Monthly	Implemented
4.5.3	Stressed-exit and substitutability shall be considered for concentrate…	TPRM	Quarterly	Implemented
4.5.4	Contractual flow-down of security and notification obligations to sub-…	APRA CPS 230	Annual	Implemented

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

Appendix A — Control implementation checklist

Control area	Controls	Implementation status
Onboarding and due diligence	3 control(s)	Implemented
Ongoing monitoring	3 control(s)	Implemented
Concentration and exit	3 control(s)	Implemented
Cloud and SaaS provider governance	4 control(s)	Implemented
Fourth-party and concentration risk	4 control(s)	Implemented
Governance, accountability and policy lifecycle	4 control(s)	Implemented

Control area	Controls	Implementation status
Risk assessment and treatment	4 control(s)	Implemented
Monitoring, measurement and reporting	4 control(s)	Implemented
Records, retention and evidence	4 control(s)	Planned
Continuous improvement	3 control(s)	Partially implemented

Appendix B — Control testing and evidence matrix

Control area	Ctrls	Test method	Evidence	Frequency
Onboarding and due diligence	3	Configuration review + sampling	Config export + screenshots	Quarterly
Ongoing monitoring	3	Automated control telemetry	Dashboard / telemetry extract	Annual
Concentration and exit	3	Evidence inspection + interview	Approved records + tickets	Annual
Cloud and SaaS provider governance	4	Re-performance / observation	Observed run + sign-off	Quarterly
Fourth-party and concentration risk	4	Log and exception review	SIEM / log extract	Semi-annual
Governance, accountability and policy lifecycle	4	Independent test / scan	Scan / test report	Monthly
Risk assessment and treatment	4	Configuration review + sampling	Config export + screenshots	Quarterly
Monitoring, measurement and reporting	4	Automated control telemetry	Dashboard / telemetry extract	Annual
Records, retention and evidence	4	Evidence inspection + interview	Approved records + tickets	Annual
Continuous improvement	3	Re-performance / observation	Observed run + sign-off	Semi-annual

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

13. Document approval and distribution

Approval	Name	Role	Date
Prepared by	Greg Thompson	Network Security Lead	10 Oct 2026
Reviewed by	James O'Connor	Head of Operational Risk	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

Abbreviation	Meaning
SIEM / SOC	Security Information & Event Management / Security Operations Centre

15. Revision history

Version	Date	Author	Summary of change
1.0	03 Oct 2024	Mei-Lin Tan	Initial issue.
2.4	02 Oct 2025	Priya Sharma	Annual review; control uplift and framework alignment.