Southern Mutual Bank

51 824 753 556

Disaster Recovery Plan

Plan · synthetic assessor-grade test document

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

Document ID	SOU-PLN-0013
Version	2.3
Owner	David Okafor (Head of Compliance)
Approved by	CISO
Classification	Internal Use Only
Status	Approved — In force
Effective date	14 Mar 2026
Next review	14 Mar 2027

1. Purpose and control objectives

This plan establishes the requirements, accountabilities and control objectives for disaster recovery plan across Southern Mutual Bank (“the Bank”). It forms part of the Bank's Information Security Management System and supports its obligations under APRA CPS 230, ISO/IEC 27001:2022, ASD ISM. It applies to Core banking platform and supporting services.

Control objectives:

• Maintain delivery of critical operations within tolerance through disruption.

• Recover systems and data within agreed objectives and demonstrate this through testing.

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

4. Requirements

4.1 Critical operations and tolerances

4.1.1 Critical operations shall be identified end-to-end (people, process, technology, third parties) and approved by the Board.

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

4.1.2 Tolerance levels for disruption shall be set for each critical operation and monitored.

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

4.1.3 Recovery time objectives (RTO) and recovery point objectives (RPO) shall be defined per critical system.

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

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

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

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

4.2 Backup and recovery

4.2.1 Backups shall be performed on a defined schedule, encrypted, and stored with at least one immutable/offline copy (3-2-1-1).

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

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

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

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

4.2.2 Restoration tests shall be performed at least annually for critical systems with results evidenced.

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

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

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

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

4.2.3 Backup failures shall be alerted and remediated within defined timeframes.

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

4.3 Continuity and scenario testing

4.3.1 Disaster-recovery plans shall be maintained and exercised for critical systems at least annually.

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

4.3.2 Severe-but-plausible scenarios (incl. cyber and third-party failure) shall be tested and lessons fed back.

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

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

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

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

4.3.3 Business continuity arrangements shall address workforce, workplace, technology and supplier dependencies.

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

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

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

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

4.4 Backup architecture and immutability

4.4.1 Backups shall follow a 3-2-1-1 architecture with at least one immutable or offline copy protected from ransomware.

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

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

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

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

4.4.2 Backup scope shall cover all critical systems and data, with encryption in transit and at rest.

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

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

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

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

4.4.3 Backup success shall be monitored and failures remediated within defined timeframes.

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

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

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

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

4.4.4 Recovery from backup shall be tested at least annually with results evidenced.

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

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

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

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

4.5 Scenario testing and exercising

4.5.1 Severe-but-plausible scenarios (cyber, third-party, data-centre and key-personnel loss) shall be tested at least annually.

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

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

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

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

4.5.2 Exercises shall include tabletop and, for critical operations, live or simulated failover.

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

4.5.3 Lessons learned shall be logged and improvement actions tracked to closure.

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

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

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

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

4.5.4 Tolerances for disruption shall be validated against exercise outcomes and updated as needed.

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 Compliance. *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. re-performance / observation. *Frequency.* Annual. *Control owner.* Head of Compliance. *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.* Monthly. *Control owner.* Head of Compliance. *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.* Quarterly. *Control owner.* Head of Compliance. *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. log + exception review. *Frequency.* Monthly. *Control owner.* Head of Compliance. *Status.* Implemented (self-declared by the document author; not independently verified).

4.7 Risk assessment and treatment

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

automated workflow and logging.

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

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

4.9 Records, retention and evidence

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

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

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

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

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

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

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

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

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

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

4.10 Continuous improvement

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

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

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

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

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

5. Roles and responsibilities (RACI)

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

6. Procedures and implementation

6.1 Maintain the critical-operations register and dependency map; review after material change.

6.2 Run scheduled backups; execute and evidence annual restoration and DR tests.

6.3 Conduct scenario / tabletop exercises; capture and track improvement actions.

7. Monitoring, metrics and KPIs

Metric	Target	Frequency
Critical systems with tested DR plan	100%	Annual
Successful restoration tests	100%	Annual
Backup success rate	≥ 99%	Monthly
Critical operations within tolerance	100%	Quarterly

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
RTO / RPO	Maximum acceptable time to recover / maximum acceptable data loss.
Tolerance level	The maximum acceptable level of disruption to a critical operation.
3-2-1-1 backup	Three copies, two media, one offsite, one immutable/offline.

11. Related documents

- Operational Resilience Policy (CPS 230)
- Disaster Recovery Plan
- Backup & Restoration Standard

12. Control framework mapping

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

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: Maintain delivery of critical operations within tolerance through disruption.
- Risk addressed: Recover systems and data within agreed objectives and demonstrate this through testing.

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	Critical operations shall be identified end-to-end (people, process, t…	APRA CPS 230	Quarterly	Implemented
4.1.2	Tolerance levels for disruption shall be set for each critical operati…	ISO/IEC 27001:2022	Quarterly	Implemented
4.1.3	Recovery time objectives (RTO) and recovery point objectives (RPO) sha…	ASD ISM	Annual	Partially implemented
4.2.1	Backups shall be performed on a defined schedule, encrypted, and store…	APRA CPS 230	Monthly	Implemented
4.2.2	Restoration tests shall be performed at least annually for critical sy…	ISO/IEC 27001:2022	Quarterly	Implemented
4.2.3	Backup failures shall be alerted and remediated within defined timefra…	ASD ISM	Annual	Implemented
4.3.1	Disaster-recovery plans shall be maintained and exercised for critical…	APRA CPS 230	Semi-annual	Partially implemented
4.3.2	Severe-but-plausible scenarios (incl. cyber and third-party failure) s…	ISO/IEC 27001:2022	Quarterly	Implemented
4.3.3	Business continuity arrangements shall address workforce, workplace, t…	ASD ISM	Annual	Implemented
4.4.1	Backups shall follow a 3-2-1-1 architecture with at least one immutabl…	APRA CPS 230	Quarterly	Implemented
4.4.2	Backup scope shall cover all critical systems and data, with encryptio…	ISO/IEC 27001:2022	Quarterly	Implemented
4.4.3	Backup success shall be monitored and failures remediated within defin…	ASD ISM	Quarterly	Partially implemented
4.4.4	Recovery from backup shall be tested at least annually with results ev…	APRA CPS 230	Annual	Implemented
4.5.1	Severe-but-plausible scenarios (cyber, third-party, data-centre and ke…	ISO/IEC 27001:2022	Semi-annual	Partially implemented
4.5.2	Exercises shall include tabletop and, for critical operations, live or…	ASD ISM	Monthly	Partially implemented
4.5.3	Lessons learned shall be logged and improvement actions tracked to clo…	APRA CPS 230	Monthly	Implemented
4.5.4	Tolerances for disruption shall be validated against exercise outcomes…	ISO/IEC 27001:2022	Monthly	Implemented

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

Appendix A — Control implementation checklist

Control area	Controls	Implementation status
Critical operations and tolerances	3 control(s)	Implemented
Backup and recovery	3 control(s)	Implemented
Continuity and scenario testing	3 control(s)	Implemented

Control area	Controls	Implementation status
Backup architecture and immutability	4 control(s)	Planned
Scenario testing and exercising	4 control(s)	Partially implemented
Governance, accountability and policy lifecycle	4 control(s)	Implemented
Risk assessment and treatment	4 control(s)	Planned
Monitoring, measurement and reporting	4 control(s)	Implemented
Records, retention and evidence	4 control(s)	Implemented
Continuous improvement	3 control(s)	Implemented

Appendix B — Control testing and evidence matrix

Control area	Ctrls	Test method	Evidence	Frequency
Critical operations and tolerances	3	Configuration review + sampling	Config export + screenshots	Monthly
Backup and recovery	3	Automated control telemetry	Dashboard / telemetry extract	Monthly
Continuity and scenario testing	3	Evidence inspection + interview	Approved records + tickets	Quarterly
Backup architecture and immutability	4	Re-performance / observation	Observed run + sign-off	Monthly
Scenario testing and exercising	4	Log and exception review	SIEM / log extract	Monthly
Governance, accountability and policy lifecycle	4	Independent test / scan	Scan / test report	Semi-annual
Risk assessment and treatment	4	Configuration review + sampling	Config export + screenshots	Annual
Monitoring, measurement and reporting	4	Automated control telemetry	Dashboard / telemetry extract	Monthly
Records, retention and evidence	4	Evidence inspection + interview	Approved records + tickets	Semi-annual
Continuous improvement	3	Re-performance / observation	Observed run + sign-off	Annual

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

13. Document approval and distribution

Approval	Name	Role	Date
Prepared by	David Okafor	Head of Compliance	10 Oct 2026
Reviewed by	Laura Mendez	Third-Party Risk Manager	20 Oct 2026
Approved by	Priya Sharma	Chief Information Security Officer	26 Oct 2026
Endorsed by	—	Board Risk Committee	30 Oct 2026

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

14. Abbreviations

Abbreviation	Meaning
ISMS	Information Security Management System
MFA / SSO	Multi-Factor Authentication / Single Sign-On
PAM / IGA	Privileged Access Management / Identity Governance & Administration
RTO / RPO	Recovery Time Objective / Recovery Point Objective

Abbreviation	Meaning
SoD	Segregation of Duties
KRI / KPI	Key Risk Indicator / Key Performance Indicator
SIEM / SOC	Security Information & Event Management / Security Operations Centre

15. Revision history

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