Southern Mutual Bank

51 824 753 556

Incident Post-Mortem — Q3 2025

Report · synthetic assessor-grade test document

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

Report ID	SOU-RPT-0208
Prepared by	Nadia Petrova (Privacy Counsel)
Classification	Internal Use Only
Status	Final
Reporting period	Q3 2025
Distribution	Control owner; Risk & Compliance; Internal Audit

1. Scope and method

This report records the results of incident post-mortem for Southern Mutual Bank over the reporting period. Results were produced from the system of record and the tooling named below; exceptions are listed with an owner and a due date and are tracked to closure by the control owner, with second-line oversight.

2. Summary of results

Security incident	INC-2026-0142 — business email compromise, severity 2
Time to detect / contain	41 min / 2h 10m
Customer impact	None confirmed
Notifications	APRA CPS 234 within 72h; OAIC assessment — not eligible

3. Results

Timeline	Event / response action	Owner	Status
T+00:39	Lessons learned workshop	Mei-Lin Tan	Delayed — escalation path unclear
T+02:33	Recovery — service restored	Priya Sharma	Completed
T+04:29	Incident declared — severity 2	James O'Connor	Completed
T+06:13	Incident declared — severity 2	David Okafor	Delayed — escalation path unclear
T+08:50	SIEM alert — anomalous privileged logon	Tom Bauer	Completed
T+10:10	Incident declared — severity 2	Aisha Khan	Delayed — escalation path unclear
T+12:39	Incident declared — severity 2	Laura Mendez	Delayed — escalation path unclear
T+14:07	Lessons learned workshop	Daniel Wright	Completed
T+16:49	Containment — account suspended, host isolated	Nadia Petrova	Completed

Timeline	Event / response action	Owner	Status
T+18:10	Regulator notified within timeframe	Greg Thompson	Delayed — escalation path unclear

4. Findings and follow-up actions

No exceptions were identified in the period.

5. Control framework mapping

Framework	Indicative mapped controls
NDB Scheme	Assessment, Notification
APRA CPS 234	Information security capability, Control testing, Incident notification
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23

6. Review and approval

Role	Name	Date
Prepared by	Nadia Petrova	03 Nov 2026
Reviewed by (2nd line)	Priya Sharma	06 Nov 2026
Approved by	Chief Information Security Officer	08 Nov 2026