Southern Mutual Bank

51 824 753 556

Security Awareness Training Completion Report — Q2 2026

Report · synthetic assessor-grade test document

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

Report ID	SOU-RPT-0128
Prepared by	Nadia Petrova (Privacy Counsel)
Classification	Internal Use Only
Status	Final
Reporting period	Q2 2026
Distribution	Control owner; Risk & Compliance; Internal Audit

1. Scope and method

This report records the results of security awareness training completion report 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 awareness training completion	97.2% (target 98%)
Personnel overdue	61 — escalated to people leaders
Role-based training — privileged users	100%
New starters trained within 30 days	99%
Gateway administrators formally trained	14 of 14 — operation and management of gateways

3. Results

Business unit	Headcount	Completion	Overdue	Course
Retail Banking	404	93%	2	Insider threat awareness
Business Banking	644	92%	0	Security awareness training — annual
Institutional Banking	503	100%	11	Insider threat awareness
Wealth & Advice	607	91%	13	Security awareness training — annual
Operations	610	100%	8	Insider threat awareness

Business unit	Headcount	Completion	Overdue	Course
Technology	393	90%	10	Security awareness training — annual
Contractors	659	99%	9	Security awareness training — annual
Network & gateway administrators	14	100%	0	Gateway administration — system administrators for gateways are formally trained on the operation and management of gateways (firewall, email gateway, web gateway) before privileged access is granted; certificate retained

4. Findings and follow-up actions

No exceptions were identified in the period.

5. Control framework mapping

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

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