Southern Mutual Bank

51 824 753 556

Vendor Assurance Evidence (SOC 2 summary) — Microsoft — Q3 2025

Report · synthetic assessor-grade test document

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

Report ID	SOU-RPT-0206
Prepared by	Laura Mendez (Third-Party Risk Manager)
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 vendor assurance evidence (soc 2 summary) 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

Supplier	Microsoft
Report	SOC 2 Type II, 12-month period, unqualified opinion
Complementary user entity controls	7 — mapped to our controls
Sub-service organisations	2 — carve-out method

3. Results

Trust services criterion	Auditor conclusion	Exceptions	Our review
A1.2 Recovery	Operating effectively	None	Reviewed by Mei-Lin Tan
CC6.6 Boundary protection	Exception noted — management response accepted	1 — access review sample	Reviewed by Priya Sharma
CC6.6 Boundary protection	Exception noted — remediated	2 — change approval evidence	Reviewed by James O'Connor
CC7.2 Monitoring	Operating effectively	None	Reviewed by David Okafor
CC6.1 Logical access	Exception noted — management response accepted	2 — change approval evidence	Reviewed by Tom Bauer
CC7.2 Monitoring	Exception noted — management response accepted	None	Reviewed by Aisha Khan

Trust services criterion	Auditor conclusion	Exceptions	Our review
CC6.6 Boundary protection	Exception noted — management response accepted	2 — change approval evidence	Reviewed by Laura Mendez
CC7.3 Incident response	Exception noted — remediated	None	Reviewed by Daniel Wright
CC9.2 Vendor management	Exception noted — management response accepted	None	Reviewed by Nadia Petrova
CC7.3 Incident response	Operating effectively	None	Reviewed by Greg Thompson

4. Findings and follow-up actions

No exceptions were identified in the period.

5. 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

6. Review and approval

Role	Name	Date
Prepared by	Laura Mendez	03 Nov 2026
Reviewed by (2nd line)	Greg Thompson	06 Nov 2026
Approved by	Chief Information Security Officer	08 Nov 2026