Southern Mutual Bank

51 824 753 556

Penetration Test Report — Core Banking (Temenos T24) — Q2 2026

Report · synthetic assessor-grade test document

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

Report ID	SOU-RPT-0105
Prepared by	Aisha Khan (Security Operations Lead)
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 penetration test 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

Scope	Core Banking (Temenos T24) — external and authenticated penetration test of the web application, API and attack surface
Findings by severity	1 high, 4 medium, 5 low
Re-test	8 of 10 closed; vulnerability assessment and hardening actions verified
Method	OWASP WSTG / PTES penetration testing

3. Results

Ref	Finding	Severity	Weakness	Status	Owner
PT-01	Outdated component with known vulnerability	Medium	CWE-639	OPEN — risk accepted to 19 Dec 2026	Mei-Lin Tan
PT-02	Verbose error disclosure	Low	CWE-1104	Remediated and re-tested 25 Oct 2026	Priya Sharma
PT-03	Broken access control — horizontal privilege escalation	High	CWE-639	Remediated and re-tested 21 Sep 2026	James O'Connor
PT-04	Outdated component with known vulnerability	Low	CWE-639	Remediated and re-tested 28 Sep 2026	David Okafor

Ref	Finding	Severity	Weakness	Status	Owner
PT-05	Broken access control — horizontal privilege escalation	Low	CWE-209	Remediated and re-tested 21 Oct 2026	Tom Bauer
PT-06	Missing security headers	Medium	CWE-639	OPEN — risk accepted to 19 Dec 2026	Aisha Khan
PT-07	Broken access control — horizontal privilege escalation	Medium	CWE-1104	Remediated and re-tested 01 Oct 2026	Laura Mendez
PT-08	Insecure direct object reference	Low	CWE-209	Remediated and re-tested 08 Oct 2026	Daniel Wright
PT-09	Missing security headers	Low	CWE-639	Remediated and re-tested 15 Sep 2026	Nadia Petrova
PT-10	Verbose error disclosure	Low	CWE-1104	Remediated and re-tested 30 Oct 2026	Greg Thompson

4. Findings and follow-up actions

Item	Action	Owner	Due
PT-01	Remediate and evidence closure	Mei-Lin Tan	01 Jan 2027
PT-06	Remediate and evidence closure	Priya Sharma	22 Dec 2026

5. Control framework mapping

Framework	Indicative mapped controls
ASD ISM	Guidelines: Access, System hardening, Monitoring
Essential Eight	ML2 target
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23
SOC 2 (TSC)	CC6.1, CC6.2, CC6.3, CC7.2
APRA CPS 234	Information security capability, Control testing, Incident notification

6. Review and approval

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