Southern Mutual Bank

51 824 753 556

Patch Compliance 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-0112
Prepared by	James O'Connor (Head of Operational Risk)
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 patch compliance 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

Platforms in scope	Core Banking (Temenos T24) — patch management and baseline configuration compliance
Overall patch compliance	96.4%
Critical patches missing beyond SLA	4
End-of-life software instances	2 (exception EXC-002) — patching not possible, hardening compensates
Automatic software and firmware updates	Security-relevant software and firmware updates install automatically on the platforms listed (update rings enforced by platform policy); exceptions carry a manual patch window
Previous versions removed	Superseded software and firmware versions removed after the updated version installed — verified against the authorised software list; 3 hosts pending removal

3. Results

Platform	Devices	Patch compliance	Missing critical	SLA	Evidence
Windows Server 2022	123	89.1%	3	Within 48h critical / 14d high	Patch cycle 08 Nov 2026
RHEL 9	107	99.3%	0	Within 14d	Patch cycle 31 Oct 2026
RHEL 9	284	88.3%	5	Within 14d	Patch cycle 10 Oct 2026
Windows 11 endpoints	420	95.7%	4	Within 48h critical / 14d high	Patch cycle 02 Nov 2026

Platform	Devices	Patch compliance	Missing critical	SLA	Evidence
RHEL 9	201	100.4%	1	Within 14d	Patch cycle 16 Oct 2026
Oracle DB 19c	100	90.7%	1	Within 48h critical / 14d high	Patch cycle 22 Oct 2026
Cisco IOS-XE	788	100.9%	2	Within 14d	Patch cycle 20 Oct 2026
Cisco IOS-XE	585	97.1%	4	Within 48h critical / 14d high	Patch cycle 20 Oct 2026
Windows 11 endpoints	783	93.6%	3	OVERDUE — extended maintenance window	Patch cycle 27 Oct 2026
Oracle DB 19c	637	97.1%	2	Within 14d	Patch cycle 27 Oct 2026

4. Findings and follow-up actions

Item	Action	Owner	Due
Windows 11 endpoints	Remediate and evidence closure	Mei-Lin Tan	28 Nov 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	James O'Connor	03 Nov 2026
Reviewed by (2nd line)	Aisha Khan	06 Nov 2026
Approved by	Chief Information Security Officer	08 Nov 2026