Southern Mutual Bank

Backup Jobs Report — Core Banking (Temenos T24) — Q2 2026

backup report · settings read from the system of record · synthetic assessor-grade test document

Export ID	SOU-EXP-0133
System	Core Banking (Temenos T24)
Exported by	David Okafor (Head of Compliance)
Exported	09 Nov 2026 00:00
Source	management console / configuration management database
Status	Complete

1. What this export is

A backup report for Core Banking (Temenos T24): the current settings as held by the system, section by section, with the compliance status against the applicable baseline. It reports state; it does not describe intent. Settings shown as non-compliant carry a remediation ticket.

2. Backup jobs

Setting	Value	Status
Core Banking (Temenos T24) — database	Daily full, hourly incremental; backup copies of information, software and systems maintained on the backup schedule	Success — last run 02:10
Core Banking (Temenos T24) — transaction logs	Continuous log shipping; transaction recovery by journal replay tested to the last committed transaction	Success
Core Banking (Temenos T24) — application and configuration	Daily; coordinated restoration of data, applications and settings tested	Success
Financial reporting data	Backed up nightly; restoration is tested quarterly to support recovery	Success

3. Protection of backups

Setting	Value	Status
Modification and deletion	Backups protected so only backup administrators can modify or delete them	Compliant
Immutable and offline copies	Immutable object-lock copies (30 days) and offline copies against ransomware	Compliant
Alternate storage site	Backups replicated to an alternate storage site in a separate region; agreements in place for storage and retrieval of system backup information; controls equivalent to the primary site	Compliant
Separation from primary site	Alternate storage site sufficiently separated from the primary storage site (different region, 700 km) to reduce susceptibility to the same threats — fire, flood, power and regional outage	Compliant
Redundant secondary system	Redundant secondary system not collocated with the primary; activated in the last exercise without loss of information or disruption	Compliant
Recovery components	System components used for recovery and reconstitution protected: hardened, access-restricted, monitored	Compliant

Setting	Value	Status
Environmental protections	Backup and recovery infrastructure with redundancy; environmental protections at both sites	Compliant

4. Restoration and recovery testing

Setting	Value	Status
Restore test	Restoration drill passed 12 days ago — data restored to test systems; recovery time objective met	Pass
Recovery plan procedures	Recovery plan procedures tested; disaster recovery exercise report on file	Pass
Alternate telecommunication services	Alternate telecommunication services tested quarterly	Pass
Backup retention	Retention per the records retention schedule; backup media inventory reconciled	Compliant

5. Control framework mapping

Framework	Indicative mapped controls
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
ASD ISM	Guidelines: Access, System hardening, Monitoring

Exported from the management console; integrity hash recorded in the evidence register. Reviewed by the control owner and second-line risk.