Southern Mutual Bank

Privileged Access Configuration Export — PAM Platform

configuration export · settings read from the system of record · synthetic assessor-grade test document

Export ID	SOU-EXP-1229
System	PAM Platform
Exported by	Greg Thompson (Network Security Lead)
Exported	09 Nov 2026 00:00
Source	management console / configuration management database
Status	Complete

1. What this export is

A configuration export for PAM Platform: 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. Privileged access management platform — configuration

Setting	Value	Status
Privileged accounts vaulted	218 of 218 privileged accounts under PAM management; credentials rotated every 30 days	Compliant
Just-in-time privileged access	Enforced — privileged access granted for a maximum of 8 hours on approved request	Compliant
Privileged access requests validated	Every request requires a business justification and approval by the system owner before privileged access is granted	Compliant
Privileged session recording	All privileged sessions recorded and retained 12 months	Compliant
Privileged accounts — internet access	Blocked — privileged accounts cannot access the internet, email or web services	Compliant
Separate privileged operating environment	Privileged users use a separate privileged workstation for administrative tasks	Compliant
Unprivileged accounts cannot logon to privileged environments	Enforced	Compliant
Privileged access revalidation	Privileged access disabled after 45 days of inactivity and revalidated annually by the system owner	Compliant

3. Privileged access event logging

Setting	Value	Status
Privileged access events logged	Yes — privileged access events, privileged account and group management events logged centrally and forwarded to the SIEM	Compliant
Credential manager and PAM audit log	Protected from unauthorised modification and deletion; monitored	Compliant
Break-glass usage alerting	Alert to the security operations centre on any use	Compliant
Least privilege — role definitions	42 privileged roles defined; access control rights reviewed quarterly	Compliant

4. Control framework mapping

Framework	Indicative mapped controls
APRA CPS 234	Information security capability, Control testing, Incident notification
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

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