Southern Mutual Bank

Secure Configuration Export — Payments Switch

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

Export ID	SOU-EXP-0222
System	Payments Switch
Exported by	James O'Connor (Head of Operational Risk)
Exported	09 Nov 2026 00:00
Source	management console / configuration management database
Status	Complete

1. What this export is

A configuration export for Payments Switch: 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. System security parameters

Setting	Value	Status
Secure configuration baseline applied	CIS Level 1 baseline for Payments Switch; system security parameters configured to prevent misuse	Compliant
Insecure services and protocols	Present: legacy FTP on host b-07 — business justification documented, additional safeguards (network isolation, monitoring) applied; retirement scheduled	Justified
Services, protocols and ports	Only approved services, protocols and ports enabled; each with a defined business need (see approved services register)	Compliant
Network security control configuration standard	Defined, implemented and maintained; firewall rule set matches the standard	Compliant
Open-source software restrictions	Approved licences only, pinned versions, vulnerability scanned before use	Compliant

3. Configuration management and verification

Setting	Value	Status
Automated configuration management	Desired-state tooling manages, applies and verifies configuration settings on every component; drift reported hourly	Compliant
Previous baseline configurations retained	3 previous versions of each baseline retained to support rollback	Compliant
Automated security response to unauthorised baseline change	Alert to SOC and automatic revert to the approved baseline	Compliant
Automatic isolation on security violation	Configurable: on defined security violations the system is automatically isolated from the network and its services stopped pending review	Compliant
Configuration control for components in service or repair	Components awaiting service or repair, and repaired components awaiting return, held under configuration control with integrity verification before return to service	Compliant

Setting	Value	Status
Alternative configuration management process	Where no dedicated developer configuration management team exists, named organisational personnel operate the change and configuration process	Compliant
Alternative security mechanisms	Supplemental mechanisms defined for use when a primary security function is unavailable or compromised (offline allowlist, break-glass logging)	Compliant

4. Information protection in shared resources and sessions

Setting	Value	Status
Information in shared system resources	Memory and storage cleared between processes and users; object reuse controls prevent unauthorised information transfer via shared resources	Compliant
Multilevel / periods processing	Documented procedures applied when processing switches between classification levels; shared resources sanitised at each switch	Compliant
Anti-spoofing of security attributes	Security attributes indicating successful application of a security process are cryptographically bound; anti-spoofing mechanisms in place	Compliant
Allowed certificate authorities	Only the organisation-defined certificate authorities are trusted for protected session establishment	Compliant
Security and privacy attributes on transmission	Classification labels and privacy attributes associated with information exchanged between systems and components	Compliant
Anti-spoofing / injection prevention	Parameterised queries, input validation and output encoding enforced; untrusted data injections prevented; software engineering techniques mitigate injection, XSS and buffer overflow	Compliant
Information output filtering	Output from Payments Switch reporting programs validated against expected content before release	Compliant
Web application firewall	Public-facing web applications protected: WAF with OWASP CRS rules in blocking mode; web-based attacks detected and prevented	Compliant

5. Endpoint and mobile code settings on this system

Setting	Value	Status
Mobile code download and automatic execution	Prevented on the application tier; actions enforced before execution	Compliant
Collaborative computing devices	Remote activation prohibited; indication of use provided	Compliant
Portable storage devices	Use of media with no identifiable owner prohibited; approved types restricted	Compliant

6. 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

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