safous

SINGAPORE COMPLIANCE CHECKLIST

Meet Singapore Compliance Requirements With Safous

Uncontrolled vendor and privileged access remain among the most common root causes of regulatory findings and incident escalation across critical infrastructure and regulated industries in Singapore.

Singapore's cybersecurity landscape spans multiple cross-sector regulations, including the Cybersecurity Act and CCoP 2.0 requirements for Critical Information Infrastructure (CII) operators, IMDA's Telecommunications Cybersecurity Code of Practice, PDPA obligations overseen by the PDPC, MAS Technology Risk Management (TRM) notices, and others.

In practice, these requirements make it essential to govern, monitor, and evidence vendor and privileged access consistently – whether work is performed on-site or under tightly controlled remote exceptions. Safous addresses this gap by providing centralized access governance and audit-ready evidence across both on-site operations and approved remote scenarios, so you can demonstrate compliance with confidence.

Safous and Singapore Regulatory Alignment

Framework	Regulation	How Safous Helps
CSA – Cybersecurity Act & CCoP 2.0: Legal framework and mandatory code for CII operators	**Cybersecurity Act (CII regime):** Requires cybersecurity audits at least once every 2 years and cybersecurity risk assessments at least once a year	Supervises vendor operations with JIT access, MFA, session recording, and exportable logs that support audits and assessments.
	CCoP 2.0 §5.1.3 – Vendor Access: Vendor access must be pre-approved, documented, supervised, and performed on-site (subject to any waiver or approval where applicable)	Supports governed vendor access (including on-site operations) through approval workflows, time-bound access, MFA, and full activity recording.
	CCoP 2.0 §5.7 – Remote Connections: Remote access disabled by default, allowed only with MFA, cryptography, secure intermediaries, file sanitization, and minimal data flows	Provides a bastionless secure access path, segmented routing, file-transfer control, and SIEM integration.
IMDA – Telecommunications Cybersecurity: Mandatory for designated telecommunications licensees	**TCCoP:** Mandates prevention, protection, detection, response, and incident management across Internet-service networks	Supports pre-approved, least-privilege remote sessions with MFA, session recording, and SIEM-ready logs.
	IoT Cybersecurity Guide: Guides lifecycle practices for IoT (voluntary unless mandated by a regulator or referenced contractually)	Records managed device access, supports policy-based restrictions on tools and access paths, and helps reduce the risk of lateral movement.
PDPC – Personal Data Protection Act (PDPA): Cross-sector data-protection framework for all organizations processing personal data in Singapore	**Data Protection Obligations:** Make reasonable security arrangements to protect personal data in the organization's possession or under its control	Applies least-privilege JIT access, MFA, and credential vaulting; logs and recordings support accountability.
	Data Breach Notification: For notifiable data breaches, organizations must notify PDPC as soon as practicable, and no later than 3 calendar days after determining notifiability, and notify affected individuals as soon as practicable	Provides real-time alerts, time-sequenced logs, and exportable evidence to speed up notification workflows.

Framework	Regulation	How Safous Helps
	Transfer Limitation: Requires comparable protection for outbound transfers	Enforces geo-segmented access, file-transfer controls, and auditable session logs to restrict data flows.
	DPTM SS 714:2025: PDPA-aligned national standard for accountable DP practices	Centralizes controls, approvals, and logs into assessor-ready reports to support certification.
SS 584:2020 – Multi-Tier Cloud Security (MTCS): Cloud-security standards for all organizations processing personal data in Singapore	**SS 584:2020 Tiers 1–3:** Certification & public listing used in procurement	Provides a central platform for multi-cloud privileged operations with activity logs and policy-segmented access paths.
GovTech – IM8: Consolidated standards for government ICT	**ICT&SS Policy Reform:** Government agencies must implement right-fit risk controls and produce System Security Plan (SSP) evidence	Uses time-bounded privilege elevation and tamper-evident recordings to support SSP evidence and third-party oversight.
MOH – Cyber & Data Security: Guidelines for healthcare providers	**Guidelines (2023) & Guidebook (2025):** Outlines standards for HIB-aligned controls	Supports JIT/MFA-controlled vendor access, full session recording, and evidence exports for audits and investigations.
CSA – Cyber Essentials & Cyber Trust: Foundational and advanced controls for all organizations processing personal data in Singapore	**Cyber Essentials & Cyber Trust Marks:** Security requirements for IT, cloud, OT, and AI	Segmented and supervised remote operations with MFA, least-privilege policies, and complete access traceability.
MAS – TRM Guidelines & Notices: Principles and mandatory notices for MAS-regulated financial institutions	**TRM Guidelines (2021):** Principles for secure privileged & remote access, logging/audits, and third-party governance	Enables JIT, RBAC, and MFA for vendors, session recording with integrity logs, and centralized policy control.
	Notice FSM-N05: Mandatory root cause analysis report for applicable events within 14 days	Time-sequenced logs and session recordings accelerate root cause analysis and notification reporting.
	Notice FSM-N06: Secure admin accounts, baseline patching, and credential hygiene	Enforces MFA for admins, removes shared credentials with vaulting, and records change sessions to operationalize hygiene.

Simplify Cross-Sector Compliance in Singapore With Safous

Safous makes it easy to enforce secure, policy-based remote access by combining just-in-time controls, credential vaulting, enforced MFA, full-session recording, SIEM integration, and much more in a modern, cloud-based platform – so Singaporean organizations have a clear path to implementing and evidencing the required controls.

Talk to our team today to see how Safous can help you simplify cross-sector compliance.

EXPLORE SAFOUS

Disclaimer: Safous supports implementation and evidence of controls; it does not itself constitute compliance or replace required approvals or processes.