safous

PHILIPPINES COMPLIANCE CHECKLIST

Meet Philippines Compliance Requirements With Safous

Philippine regulations – including the Philippines National Cybersecurity Plan (NCSP 2023–2028), Bangko Sentral ng Pilipinas Enhanced Guidelines on Information Security Management (BSP Circular No. 982, Series of 2017), RA 10844 (DICT Act), RA 10173 (Data Privacy Act), ISO/IEC 27001/27002/27011, and IEC 62443 – collectively aim to build a secure and resilient digital ecosystem. Together, they emphasize on protecting personal and sensitive data, strengthening cybersecurity governance, and promoting consistent security practices across both the public and private sectors.

Safous helps organizations in the Philippines meet local regulatory and international cybersecurity standards with a unified platform that enables secure, auditable, and policy-based remote access – without relying on legacy VPNs.

Safous and Philippine Regulatory Alignment

Framework	Regulation	How Safous Helps
Philippines National Cybersecurity Plan (NCSP 2023–2028)	NCSP 2023–2028 – Outcome 1: Strengthen protection of government networks; enable coordinated detection and incident handling.	Enforces least-privilege admin access, records sessions for forensics, and integrates with SIEM/NCERT feeds.
BSP Circular No. 982 (Series of 2017)	BSP Circular No. 982 – Incident analysis & forensic readiness: Timely triage, containment, notification to BSP, and forensic-ready logs.	Provides indexed session recordings, immutable logs, and integration with SIEM for fast triage & reporting.
	BSP Circular No. 982 – Third-party/cloud outsourcing oversight: Financial institutions retain oversight; must enforce controls on vendors.	Centralizes control of outsourced vendor access, time-boxed and approved sessions, and vendor-specific audit logs.
RA 10844 (DICT Act of 2015)	RA 10844 – DICT IRR: Implement network security and secure remote access for government systems.	Provides supervised vendor access work-flows, approvals, and detailed audit trails.
RA 10173 (Data Privacy Act of 2012)	RA 10173 – Sec. 20: Implement organizational, physical, and technical measures to protect personal data.	Enforces RBAC, MFA, encryption, and detailed session recording to control and audit data access.
	RA 10173 – Sec. 21: Implement breach detection, logging, and incident response measures.	Provides real-time logging, alerts, and exportable forensic evidence for NPC breach notification compliance.
	RA 10173 – Sec. 32/100–101: Implement appropriate measures; notify NPC and subjects of harmful breaches.	Enables credential vaulting, MFA, and RBAC to reduce breach risk, and forensic evidence/logs enable NPC notifications.

Safous and Philippine Regulatory Alignment

Framework	Regulation	How Safous Helps
ISO/IEC 27001	ISO/IEC 27001 – A.9: Restrict access to systems based on business and security needs.	Implements least privilege, role-based access, and JIT session approval workflows.
	ISO/IEC 27001 – A.12: Ensure secure operations and logging for accountability.	Records all privileged sessions with immutable logs and command history for audit purposes.
IEC 62443 (ISA/IEC 62443 Series)	IEC 62443-2-4: Service providers must ensure secure remote access and monitoring.	Enables supervised, approved remote sessions with detailed logs for OT systems.
	IEC 62443-3-3: Segment networks into zones and control data flow between them.	Applies zone-based access policies and encrypted conduits to enforce network segregation.

Simplify Compliance in the Philippines With Safous

Safous brings least-privilege access, just-in-time access, credential vaulting, MFA integration, privileged session recording, tamper-proof audit trails, and SIEM integration together in a cloud-based, modern platform – so Philippine organizations can meet regulatory requirements with confidence.

Talk to our team today to see how Safous can support your compliance goals.

EXPLORE SAFOUS