safous

TAIWAN COMPLIANCE CHECKLIST

Meet Taiwan Regulatory Requirements With Safous

Taiwan's cybersecurity and data protection framework is based on a layered regulatory model. Statutory laws such as the Personal Data Protection Act (PDPA) and the Cyber Security Management Act (CSMA) establish high-level obligations, while enforcement rules, reference standards, and sector-specific expectations define how these obligations are implemented and assessed in practice.

For organizations operating critical infrastructure and industrial OT environments, compliance is evaluated not only against legal provisions but also against operational governance, third-party access control, and auditability of privileged activities.

Safous supports these requirements through secure, identity-centric, and fully auditable remote access across IT and OT environments – without reliance on legacy VPN architectures.

Safous and Taiwan Regulatory Alignment

LAYER 1: STATUTORY LAWS

Regulation	Article/ Clause	Requirement	Applicability	How Safous Helps
PDPA	Art. 27	Implement appropriate security measures to protect personal data	Non-government organizations	MFA, RBAC, least-privilege access, encrypted sessions, audit logs
PDPA	Art. 18	Secure the maintenance and management of personal data	Government agencies	Identity-centric access, session traceability
PDPA	Art. 12	Notify data subjects after breach facts are clarified	All PDPA-regulated entities	Session evidence, investigation support
CSMA	Chapters 2–3	Establish cybersecurity governance and security planning	Government agencies & designated critical operators	Centralized access governance, policy enforcement

LAYER 2: CSMA ENFORCEMENT RULES

Regulation	Enforcement Rule	Requirement	How Safous Helps
PDPA	Art. 6(1)	Cybersecurity risk assessment	Visibility into privileged access paths
PDPA	Art. 6(2)	Protective and control measures	MFA, RBAC, just-in-time access, approvals
PDPA	Art. 6(3)	Incident reporting and response	Session recording, real-time alerts
PDPA	Art. 6(4)	Threat intelligence monitoring	SIEM integration, session analytics
PDPA	Art. 6(5)	Outsourcing and third-party management	Vendor-scoped access, no standing VPNs

LAYER 3: STANDARDS AND REFERENCE FRAMEWORKS

Standard/ Guideline	Relevant Control	Requirement	How Safous Helps
NICS Guidance	Implementation references	Practical reference for CSMA compliance	Dashboards, reports, immutable logs
IEC 62443-3-3	SR 1.1	Human user identification and authentication	MFA for OT engineers
IEC 62443	Remote maintenance principles	Secure and auditable OT access	Brokered access, session recording
IEC 62443	Remote maintenance principles	Secure and auditable OT access	Brokered access, session recording

LAYER 4: INDUSTRY-SPECIFIC PRACTICAL REQUIREMENTS

Industry	Source Regulation	Requirement	How Safous Helps
Energy/ Utilities	CSMA Enforcement Rules Art. 6(2)	Strict control of remote access to operational systems	MFA, identity-based access
Energy/ Utilities	CSMA Enforcement Rules Art. 6(5)	Governance of vendor and maintenance access	Just-in-time vendor access
Transport	CSMA Enforcement Rules Art. 6(3)	Ability to reconstruct access-related incidents	Session recording, forensic logs
Telecom	NICS Guidance + CSMA	Continuous monitoring and audit readiness	Centralized logs, SIEM integration

LAYER 4: INDUSTRY-SPECIFIC PRACTICAL REQUIREMENTS

Industry	Source Regulation	Requirement	How Safous Helps
Semiconductor	IEC 62443-3-3 SR 1.1	Secure remote maintenance for production systems	MFA-based OT access
Semiconductor	IEC 62443 audit principles	Traceability of engineering actions	Session-level recording
Manufacturing (OT)	CSMA Enforcement Rules Art. 6(2)	Restricted network exposure during remote access	Brokered access without VPN
Manufacturing (OT)	CSMA Enforcement Rules Art. 6(5)	Governance of outsourced engineers	Time-bound, task-scoped access

Disclaimer: This document is for informational purposes only and is not legal or regulatory advice. Regulatory requirements and interpretations (including PDPA and CSMA) may vary and change; organizations should consult qualified Taiwan legal or compliance advisors before relying on this information.

Streamline Compliance in Taiwan With Safous

Safous aligns with Taiwan's compliance landscape by addressing how regulatory requirements are actually assessed in practice, from legal obligations and enforcement rules to industry-specific audit expectations. By providing secure, identity-centric, and fully auditable remote access across IT and OT environments, Safous enables organizations to demonstrate compliance with confidence – while reducing operational and third-party access risk.

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

EXPLORE SAFOUS

safous