

How Privileged Remote Access Helps Critical Infrastructure Operators Achieve Compliance

safous

Table of Contents

03 Executive Summary

04 Compliance Across the APAC Region

06 What Is Privileged Remote Access (PRA)?

07 How PRA Aligns With Compliance Frameworks

08 Use Case: PRA in Critical Infrastructure

09 Benefits of PRA Beyond Compliance

10 Achieve Compliance With Safous PRA



Executive Summary

Governments across Southeast Asia are taking a stronger stance on cybersecurity, especially when it comes to critical infrastructure. With new laws and frameworks in countries like Malaysia and Thailand setting stricter requirements for how essential service providers secure access to their systems, businesses must be more proactive about managing who can access what.

A 2025 report found that **72% of APAC organizations plan to increase their cybersecurity spending this year.**[1] For many, that includes investing in solutions like Privileged Remote Access (PRA) to manage privileged access securely and in line with regulatory frameworks. In this white paper, we'll examine how Privileged Remote Access – also known as Remote Privileged Access Management (RPAM) – helps critical infrastructure operators strengthen cyber resilience and simplifies compliance audits, especially in complex operational technology (OT) and hybrid IT/OT environments.

1. https://www.computerweekly.com/news/366618762/APAC-organisations-to-ramp-up-tech-spending-in-2025

Compliance Across the APAC Region



MALAYSIA'S CYBERSECURITY ACT 2024

Malaysia's Cybersecurity Act 2024, which came into effect in August 2024, mandates stronger protection of National Critical Information Infrastructure (NCII) across 11 sectors, including energy, finance, healthcare, and telecommunications.

Among the security requirements are **identity management, secured remote access, continuous monitoring, and full audit trails.** NCII business leaders who fail to comply could face penalties like suspension of licenses, fines, or imprisonment.



THAILAND'S CYBERSECURITY ACT B.E. 2562 (2019)

In Thailand, the Cybersecurity Act B.E. 2562 (2019) enables the National Cyber Security Agency of Thailand (NCSA) to enforce security guidelines for critical information infrastructure operators (CIIOs).

Per the NCSA's latest guidelines, organizations in healthcare, finance, transportation, and utilities must classify the risk level of their data/information systems and implement security measures based on the security category. Some required measures include **remote access controls, least-privilege policies, and real-time session monitoring.**

Compliance Across the APAC Region (cont.)

Several other nations across the APAC region have implemented cybersecurity frameworks to address growing digital threats, such as:



Indonesia's Personal Data Protection Law (PDP) serves as the nation's first legislation governing data protection across both electronic and non-electronic systems. It requires organizations to implement risk-based security measures to protect personal data.



Singapore's Cybersecurity Act establishes a regulatory framework for protecting critical information infrastructure. It mandates that CIIOs comply with codes of practice and standards, conduct regular cybersecurity audits, and report cybersecurity incidents.



Vietnam's Decree 53/2022/ND-CP requires organizations that process personal data or provide online services in Vietnam to store specific types of data within Vietnam and implement cybersecurity measures, including risk assessments, continuous system monitoring, and incident response planning.



The Philippines' National Cybersecurity Plan 2023-2028 emphasizes protecting critical infrastructure and fostering a culture of cybersecurity awareness by adopting strong measures like authentication systems, remote access management capabilities, and incident response.

What Is Privileged Remote Access (PRA)?

Privileged Remote Access (PRA) is a cybersecurity framework designed to provide secure, policy-based access for users with elevated privileges – such as system administrators, third-party vendors, and field engineers – especially when accessing critical infrastructure remotely.

Unlike VPNs or traditional remote desktop tools, PRA offers:



Granular access control:
Only the minimum required systems are accessible per user or session.



Session monitoring and recording:
Real-time visibility into all privileged activity.



Centralized audit logs:
Comprehensive tracking of who accessed what, when, and from where.



Credential vaulting and SSO:
Users don't need to know or handle passwords directly.



Strong authentication:
Authenticates users by MFA, device posture, or registered device.



Just-in-time (JIT) access:
Accessible only when necessary, and each access request goes to the supervisor.

When applied to OT and hybrid environments, PRA also accounts for protocol-specific access, air-gapped systems, and compliance with segmentation policies such as those in the ISA/IEC 62443 framework, which is a series of international standards for industrial cybersecurity.

How PRA Aligns With Compliance Frameworks

Here's how PRA supports compliance controls across major frameworks:

Regulation/ Standard	PRA Alignment
ISO/IEC 27001	Granular access rights, session logging, identity verification, and remote access monitoring
NIST 800-171	Least privilege, access control, session termination, and remote audit logging
GDPR	Access restriction to personal data, audit trails for access justification
PCI DSS	Role-based access to cardholder systems, encryption of credentials, session tracking
ISA/IEC 62443	IACS access management, session recording, remote session termination, and audit trail enforcement for industrial environments
HIPAA	Access controls for ePHI, technical safeguards for authentication, transmission security for remote sessions

Ultimately, PRA provides a single architecture that APAC businesses can configure to meet multi-framework compliance and strengthen their overall security posture.

USE CASES:

PRA in Critical Infrastructure

To understand Privileged Remote Access in action, here's how critical infrastructure operators might leverage these solutions to address compliance requirements:

USE CASE #1

Consider a national energy provider in Malaysia that must comply with both ISO 27001 and Malaysia's NCII-specific cybersecurity law. Implementing PRA can help the provider:

- Restrict third-party engineers' access to specific industrial control systems.
- Monitor and record privileged sessions in real time.
- Prevent credential sharing through password vaulting and one-time access tokens.
- Automatically generate audit-ready reports for compliance officers.

USE CASE #2

A large public hospital in Thailand may adopt PRA to meet the NCSA's requirements for remote access. This solution would secure access for remote maintenance vendors by enabling the organization to:

- Enforce role-based access controls for external medical device technicians.
- Create audit trails of all privileged activities for compliance reporting.
- Implement time-limited access windows for maintenance sessions.
- Block unauthorized data transfers during vendor connections.

Benefits of PRA Beyond Compliance

While regulatory compliance is a key driver of PRA, these solutions offer operational and security benefits that extend far beyond audit readiness, such as:

01 **Improved operational efficiency:**
Vendors can access necessary systems without delays or helpdesk involvement.

02 **Reduced attack surface:**
Prevents the two root causes of most ransomware incidents – over-privileged accounts and insecure remote access – to shrink the avenues through which attackers can gain entry.

03 **Incident response readiness:**
PRA's session logs and recordings accelerate forensic investigations and root cause analysis.

04 **Centralized control**
IT and security teams can manage, review, and revoke access from a single platform. Centralized management also frees them from configuration tasks that previously spanned multiple platforms, like VPNs and PAM.

05 **Scalable security architecture:**
With PRA, you can easily extend security to new sites and systems while maintaining high availability through a centrally managed architecture.



Achieve Compliance With Safous

At Safous, we designed our Privileged Remote Access platform to meet the needs of critical infrastructure operators across Southeast Asia and beyond. Our platform includes:

- Agentless access for most features, agent-based access for deeper use cases
- Multi-factor authentication (MFA)
- Session recording and real-time monitoring
- Role- and attribute-based access controls
- Air-gapped and cloudless deployment options
- Credential vaulting and just-in-time access
- No data on cloud, just routed via cloud
- Alignment with NIST, ISO, ISA/IEC 62443, PCI-DSS, and local regulations

Whether you operate in the energy, healthcare, finance, or telecom sectors, Safous PRA can help you achieve regulatory compliance – all while improving your security posture.

Ready to simplify your path to compliance and secure your infrastructure?
Contact us today to schedule a demo or compliance consultation.

