safous

ISO/IEC 27001 COMPLIANCE CHECKLIST

Simplify ISO/IEC 27001 Compliance With Safous Privileged Remote Access

ISO/IEC 27001 provides a globally recognized framework for managing information security risks – and privileged access and remote connectivity are two of its most critical control areas.

Safous Privileged Remote Access helps organizations align with ISO/IEC 27001 by enforcing identity-based access, securing remote sessions, and simplifying audit reporting. Whether you operate in IT, OT, or hybrid environments, Safous supports your compliance journey without overcomplicating your operations.

Safous Privileged Remote Access and ISO/IEC 27001 Alignment

ISO/IEC 27001 Requirement	How Safous Helps You Comply
☐ **5.8 –** Information security in projects	Enforces access control policies in IT/OT projects through centralized access provisioning.
☐ **5.9 –** Inventory of assets	Session and access logs help track which users accessed specific systems and applications.
☐ **5.15 –** Access control	Maps granular, identity-based access rules to user roles and applications.
☐ **5.16 –** Identity management	Integrates with identity providers and enforces MFA and least privilege.
☐ **5.17 –** Authentication information	Supports MFA, password vaulting, and secure SSO for privileged sessions.
☐ **5.18 –** Access rights	Allows Just-In-Time (JIT) access provisioning and approval-based workflows.
☐ **5.19 –** Supplier relationship security	Ensures secure, auditable access for vendors and third parties with session monitoring.
☐ **5.20 –** Supplier agreements	Access policies and approval workflows support the enforcement of supplier-level access agreements.
☐ **5.21 –** ICT supply chain security	Tracks and controls remote access to critical infrastructure across supplier environments.

ISO/IEC 27001 Requirement	How Safous PRA Helps You Comply
☐ **5.22 –** Supplier services monitoring	Monitors and records all third-party privileged access for audit and oversight.
☐ **5.23 –** Cloud service security	Applies consistent access policies to cloud and on-prem environments through a unified interface.
☐ **5.26 –** Information security incident response	Real-time alerts, session termination, and session logs support containment and forensics.
☐ **5.28 –** Evidence collection	Records complete session details, user actions, and timestamps for post-incident investigations.
☐ **5.30 –** Business continuity readiness	Enables secure access to critical systems during disruption with session continuity.
☐ **5.31 –** Legal and regulatory requirements	Provides audit logs and compliance reports to support regulatory documentation.
☐ **5.33 –** Protection of records	Records and stores all session logs, user actions, and access events for traceability.
☐ **5.34 –** Protection of PII	Enforces secure access policies that help prevent unauthorized exposure of PII.
☐ **5.36 –** Policy compliance	Centralizes security policy enforcement and logs deviations for accountability.
☐ **5.37 –** Documenting operating procedures	Supports documented procedures by controlling and fully auditing access to systems.
☐ **6.5 –** Post-employment access controls	Automatically removes access permissions upon role changes or termination.
☐ **6.7 –** Remote working security	Enforces VPN-less, context-aware secure remote access for internal users and external vendors.
☐ **8.1 –** Endpoint device control	Enforces device posture checks to block untrusted or non-compliant endpoints.
☐ **8.2 –** Privileged access rights	Limits privileged access through policy-based controls and strong authentication.
☐ **8.3 –** Information access restriction	Microsegmentation ensures users only reach approved applications, not networks.
☐ **8.4 –** Access to source code	Restricts access to source code unless explicitly allowed through policy controls.
☐ **8.5 –** Secure authentication	Applies strong authentication with MFA, SSO, and IdP integrations.

ISO/IEC 27001 Requirement	How Safous PRA Helps You Comply
☐ **8.7 –** Protection against malware	Browser isolation and endpoint posture checks reduce risk during privileged sessions.
☐ **8.15 –** Session logging	Logs every session in detail with user actions and time stamps.
☐ **8.16 –** Monitoring activities	Provides real-time activity monitoring and alerting for suspicious behavior.
☐ **8.20 –** Network security	Stops lateral movement through application-layer access controls and microsegmentation.
☐ **8.21 –** Network service security	Restricts traffic by protocol, port, and identity using policy-based access controls.
☐ **8.22 –** Network segregation	Application-level access avoids broad network exposure, supporting strong segmentation.
☐ **8.23 –** Web filtering	Enforces browser isolation to prevent exposure to risky external web content.
☐ **8.24 –** Use of cryptography	Applies end-to-end encrypted communication between users and resources.
☐ **8.26 –** Application security	No application code changes required; access is secured at the perimeter.
☐ **8.29 –** Security testing	Logs and session activity support secure change documentation and testing validation.
☐ **8.30 –** Outsourced development	Enforces access limits and approvals for external developers working on critical systems.
☐ **8.31 –** Separation of environments	Segregates access across dev, staging, and production with isolated session policies.
☐ **8.32 –** Change management	Tracks administrative activity and approvals to support change tracking and auditability.

Get Started With ISO/IEC 27001-Aligned Remote Access

Safous Privileged Remote Access brings Zero Trust principles to privileged access – reducing your attack surface, aligning with global compliance frameworks, and keeping your critical systems secure in a cloud-based, modern platform.

Contact us today to see how Safous can help you simplify ISO/IEC 27001 compliance with confidence.

EXPLORE SAFOUS