Teleport

Accelerate ISO 27001:2022 Compliance with Teleport

Contents

What is ISO 27001:2022? 3

- What Changed in ISO 27001:2022? 3

How Teleport Simplifies ISO 27001:2022 Compliance 4

- Implementing Zero Trust Access 4
- Eliminating Static Credentials 4
- Unifying Identity for Humans and Machines 5
- Monitoring and Recording Sessions in Real-Time 5
- Centralizing Audit Logging 5
- Enforcing Policy at Scale 5

How Teleport Maps to Annex A Controls 6

Ready to Simplify ISO 27001:2022 Compliance? 11

The Teleport Infrastructure Identity Platform maps to many of the security controls listed in Annex A of the ISO 27001:2022 standard.

Teleport helps organizations earn and retain compliance as infrastructure grows in complexity, the volume of identities expands, and as new technologies like AI are adopted across enterprises.

This document outlines key updates and new controls within ISO 27001:2022 and explains how Teleport helps organizations increase alignment to ISO requirements across Annex A's relevant control families.

Explore this guide to discover:

- What controls have changed or are new from ISO 27001:2013 to ISO 27001:2022
- What's inside Annex A, the implementation framework for ISO 27001
- How an Infrastructure Identity approach to implementation can simplify ISO compliance
- The specific ISO 27001:2022 controls to which Teleport helps organizations align

What is ISO 27001:2022?

ISO/IEC 27001:2022 is a widely recognized global standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), designed to help organizations establish and enhance their information security practices.

The standard outlines a structured approach to protecting sensitive data through a robust Information Security Management System (ISMS). Demonstrating compliance with ISO/IEC 27001:2022 enables organizations to certify that globally recognized security best practices are applied to the data used, owned, or stored by the organization.

What Changed in ISO 27001:2022?

ISO/IEC 27001 has long been the global benchmark for managing information security risk. The 2022 revision modernizes the framework for today's infrastructure landscape, where cloud-native architectures, remote work, and ephemeral systems are the norm.

With this update, the standard introduces new technical and operational expectations for identity assurance, access governance, privilege management, and continuous monitoring. These enhancements reflect the growing importance of themes central to Teleport's core mission, including Zero Trust access models, security controls for non-human identities, and a unified security posture across multi-cloud and hybrid environments.

This document outlines key updates and new controls within ISO 27001:2022 and explains how Teleport helps organizations increase their alignment to ISO requirements across Annex A's relevant control families.

Inside ISO 27001 Annex A

Annex A defines the control set that powers an Information Security Management System (ISMS), now expanded to 93 controls across four updated domains:

- **Organizational: Section 5.x**
  Governance, risk, and oversight
- **People: Section 6.x**
  Access control, roles, and responsibilities
- **Physical: Section 7.x**
  Physical protection and facilities
- **Technological: Section 8.x**
  Identity, access, logging, and systems protection

Organizations must adopt or justify each control through formal risk assessments, increasing pressure to demonstrate robust, consistent, and scalable enforcement mechanisms.

How Teleport Simplifies ISO 27001:2022 Compliance

By unifying identity, access control, and auditing, Teleport helps organizations bridge the gap between ISO 27001:2022's security controls and the day-to-day realities of managing complex cloud-native and hybrid environments, all while simplifying the audit process and the path towards certification. This is accomplished by:

- **Implementing Zero Trust Access**
- **Eliminating Static Credentials**
- **Unifying Identity for Humans and Machines**
- **Monitoring and Recording Sessions in Real-Time**
- **Centralizing Audit Logging**
- **Enforcing Policy at Scale**

Implementing Zero Trust Access

ISO 27001:2022 emphasizes the core tenets of Zero Trust — identity verification, strict access governance, and secure resource access based on contextual trust rather than static network location — through revised controls like:

- Control 5.15 - Access Control
- Control 5.16 - Identity Management
- Control 8.1 - User Endpoint Devices
- Control 8.23 - Information Security for Use of Cloud Services

Teleport helps organizations align with ISO and Zero Trust principles by enforcing identity-bound access for every human and machine interaction, issuing short-lived certificates at runtime, and applying role-based access controls across cloud, on-prem, and hybrid environments.

Whether it's a developer accessing a Kubernetes cluster or a microservice requesting secrets, access is enforced using ephemeral credentials and policy-defined constraints. Teleport enables infrastructure teams to define fine-grained permissions across users and workloads, including session timeouts, required device posture, or task-based context, supporting ISO controls for areas like remote access, authentication, and network protection.

Eliminating Static Credentials

One of the most impactful changes in ISO 27001:2022 is the emphasis on eliminating standing privileges and minimizing reliance on long-lived credentials, reflected in updated controls such as:

- Control 5.15 - Access Control
- Control 5.16 - Identity Management
- Control 8.2 - Privileged Access Rights
- Control 8.3 - Information Access Restriction

Teleport helps organizations align with these requirements by replacing passwords, SSH keys, and API tokens with short-lived, cryptographically signed certificates issued by a built-in certificate authority.

Each identity, whether a person, machine, workload, or AI agent, is assigned a trusted, verifiable identity that expires automatically. This eliminates persistent access paths, reduces the attack surface, and brings authentication in line with Zero Trust principles.

With Teleport, access is governed through granular RBAC and ABAC policies, ensuring every session is tied to a validated identity and provisioned only when needed. Engineers, workloads, and CI/CD pipelines receive time-bound access aligned to their specific role or task, eliminating the risk of over-privileged accounts — which aligns to ISO requirements for identity assurance, privilege restriction, and traceability.

Unifying Identity for Humans and Machines

Teleport delivers consistent policy enforcement and lifecycle controls for human and non-human identities. From one platform, teams can:

- Run automated access reviews (Control 5.17 - Authentication Information);
- Require approvals for privileged access (Control 8.2 - Privileged Access Rights); and
- Enforce device trust (Control 8.1 - User Endpoint Devices)

Integration with common tools like Slack, Jira, ServiceNow, and Microsoft Teams makes access governance intuitive for infrastructure teams. Engineers can request just-in-time (JIT) access from their existing workflows, while approvers gain contextual insight to enforce least privilege. Real-time enforcement of identity governance simplifies compliance and reduces audit burden, especially in dynamic environments where identities, roles, and systems change rapidly.

Monitoring and Recording Sessions in Real-Time

Teleport provides real-time session monitoring and full protocol-level session recordings for all user and workload interactions, including SSH, RDP, Kubernetes, databases, and more. Security and compliance teams can observe live sessions, replay recorded activity, and intervene when needed. This encourages alignment with ISO's requirements for traceable and controllable access activity including:

- Control 5.15 - Access Control;
- Control 5.28 - Collection of Evidence; and
- Control 8.2 - Privileged Access Rights

For highly privileged operations, Teleport supports dual authorization workflows, requiring multiple team members to approve sensitive actions. This helps organizations ensure that sensitive access is tightly governed and that approval workflows reduce the risk of misuse, in alignment with:

- Control 5.3 - Segregation of Duties; and
- Control 8.2 - Privileged Access Rights.

These capabilities complement standards like FedRAMP AC-3, supporting secure, auditable control of high-risk activities.

Centralizing Audit Logging

Teleport logs every action of users, workloads, and services in a structured, tamper-evident audit trail. These logs are identity-aware, include rich contextual data (e.g., timestamp, session duration, command activity), and are easily exportable to SIEMs, SOAR tools, and threat detection platforms.

Whether demonstrating access policy enforcement during an ISO audit or conducting a root cause analysis post-incident, Teleport's centralized logging infrastructure simplifies compliance and accelerates response time. This makes it significantly easier for organizations to satisfy ISO 27001:2022 controls related to access logging, event review, and operational accountability.

This supports ISO requirements for activity review, incident response, and forensic investigation as outlined in controls like:

- Control 5.28 - Collection of Evidence; and
- Control 5.29 - Information Security During Disruption

Enforcing Policy at Scale

Teleport unifies identity-bound access across all your infrastructure, eliminating the inconsistencies and operational risks of managing siloed access systems. Integrations with identity providers (e.g., Okta, Azure AD), HR systems, and Git-based workflows allow just-in-time access based on role, team membership, or lifecycle events. By ensuring secure onboarding, offboarding, and third-party access control, Teleport supports ISO controls such as:

- Control 5.16 - Identity Management; and
- Control 5.18 - Access Rights

Teleport also ensures that every identity within your infrastructure, human or non-human, is governed by consistent controls, regardless of cloud provider, environment, or protocol. Whether it's spinning up a new microservice in Kubernetes or onboarding a contractor to a production database, organizations can maintain policy integrity at scale while reducing manual effort and human error. This helps organizations align with ISO controls including:

- Control 5.1 - Policies for Information Security;
- Control 5.2 - Information Security Roles and Responsibilities;
- Control 5.3 - Segregation of Duties; and more.

How Teleport Maps to Annex A Controls

In the following table, explore the Annex A controls where Teleport can help you align with or satisfy requirements for ISO 27001:2022 compliance.

This mapping is intended to be informational rather than prescriptive, highlighting the Teleport capabilities that can be used to meet control definitions.

Looking for technical information or encountering ISO 27001:2022 challenges?

Schedule time with our experts to explore how can simplify your compliance journey with Teleport's Infrastructure Identity Platform.

Talk to an Expert →

ISO 27001:2022 Control	Teleport Mapping
5. Organizational Controls	
5.1 - Policies for Information Security	Teleport enforces policies by controlling who can access what systems, how, and when. Detailed audit logs support policy review and demonstrate compliance across cloud and on-prem environments.
5.2 - Information Security Roles and Responsibilities	Teleport enforces access policies tied to clearly defined roles through integration with identity providers and centralized role-based access control (RBAC). This ensures users, machines, workloads, and AI agents only receive permissions appropriate to their responsibilities, maintaining alignment between organizational structure and security enforcement.
5.3 - Segregation of Duties	Teleport enables fine-grained RBAC to ensure all users are only granted the minimum permissions needed for their job functions. This enforces separation of duties by limiting cross-functional access, reducing the risk of unauthorized actions or conflicts of interest.
5.4 - Management Responsibilities	Teleport captures comprehensive audit logs to link every infrastructure access and action to a specific identity and session. This visibility enables managers to uphold accountability, review policy enforcement, and demonstrate compliance with security responsibilities.
5.7 - Threat Intelligence	Teleport generates detailed, real-time and historical audit logs that can be exported to SIEM tools for automated threat detection and analysis. This integration allows organizations to correlate session data with broader threat intelligence efforts, enhancing proactive security monitoring and response.
5.8 - Information Security in Project Management	Teleport secures infrastructure access throughout project lifecycles with role-based and attributed-based access controls, ephemeral certificates instead of static credentials, and context-aware policies. This ensures that only authorized personnel can access project resources at each stage while supporting agile and DevOps workflows.

[table continues on next page]

ISO 27001:2022 Control	Teleport Mapping
5.9 - Inventory of Information and Other Associated Assets	Teleport maintains detailed logs of all accessed infrastructure resources, including servers, databases, and applications. These access records help organizations build and maintain an up-to-date inventory of information assets and understand who interacts with each system.
5.10 - Acceptable Use of Information and Other Associated Assets	Teleport enables administrators to enforce acceptable use policies through role-based access controls and policy-defined access boundaries. Session recordings and command logs provide a complete audit trail, allowing organizations to verify proper use and investigate any violations.
5.12 - Classification of Information	Teleport allows organizations to segment sensitive systems and resources into roles and access groups based on information classification. This ensures that only users with the appropriate clearance and need-to-know can access classified or critical infrastructure assets.
5.13 - Labelling of Information	Teleport enables organizations to restrict access to designated resources containing labeled or classified data.
5.14 - Information Transfer	Teleport secures all connections between users and infrastructure using mutual TLS encryption and short-lived, identity-bound certificates. This ensures that information in transit remains confidential and protected against interception or unauthorized access.
5.15 - Access Control	Teleport implements Zero Trust access controls using role-based permissions, identity-aware policies, and time-bound certificates. This ensures that only authenticated and authorized users can access specific infrastructure resources and that all access is logged and fully auditable.
5.16 - Identity Management	Teleport unifies identity across systems through integration with SSO providers and issuing short-lived, cryptographically signed certificates. This ensures that both human and machine identities are securely authenticated, centrally managed, and attributed to approved roles.
5.17 - Authentication Information	Teleport enhances authentication strength by requiring strong, modern authentication methods such as hardware-backed keys, biometric verification, and FIDO2 passwordless login. These measures protect authentication credentials and ensure that only verified users can access critical infrastructure and no static credentials are deployed within the access chain.
5.18 - Access Rights	Teleport dynamically manages access rights through role-based policies, short-lived certificates, and identity provider integrations. Every access grant and revocation is fully logged, ensuring traceability and alignment with user responsibilities throughout their lifecycle.
5.21 - Managing Information Security in the ICT Supply Chain	Teleport secures access to infrastructure across hybrid and multi-cloud environments through encrypted tunnels, device-aware policies, and role-based controls. All interactions with ICT components are consistently authenticated, authorized, and auditable —reducing supply chain risk
5.23 - Information Security for Use of Cloud Services	Teleport unifies and secures access controls across cloud services like AWS, GCP, Azure, and Kubernetes using short-lived credentials, role-based policies, and just-in-time access. All actions across cloud environments are centrally logged and auditable, ensuring full visibility and monitoring over cloud access.

[table continues on next page]

ISO 27001:2022 Control	Teleport Mapping
5.24 - Information Security Incident Management Planning and Preparation	Teleport provides detailed session recordings, command logs, and access metadata that enable rapid incident detection, investigation, and triage. These capabilities support proactive planning and preparedness by equipping teams with the forensic tools needed to analyze and respond to security events effectively.
5.25 - Assessment and Decision on Information Security Events	Teleport captures granular session data (e.g., keystrokes, command executions), enabling security teams to assess events accurately. Detailed telemetry supports informed decision-making during incident reviews and helps determine the exact scope and blast radius of potential security breaches.
5.26 - Response to Information Security Incidents	Teleport provides real-time session monitoring and immediate termination of suspicious activity, allowing rapid response to security incidents. Full session recordings and audit trails provide incident responders with the evidence needed to take rapid targeted, and effective action.
5.27 - Learning from Information Security Incidents	Teleport generates replayable session recordings and immutable audit logs that allow teams to perform thorough post-incident analysis. These insights can be used to identify root causes, uncover posture weaknesses, and guide improvements to security policies and response processes.
5.28 Collection of Evidence	Teleport collects and generates non-repudiable, timestamped logs and full session recordings for every access event across systems. This supplies an unimpeachable evidence trail that simplifies forensic investigations and audit proceedings.
5.29 Information Security During Disruption	Teleport maintains secure remote access to infrastructure during outages or operational disruptions. This promotes operational continuity by allowing authorized personnel to manage systems from any location without compromising security.
5.30 ICT Readiness for Business Continuity	Teleport's identity-bound access and session logging remain operational across distributed environments, supporting resilient continuity practices.
6. People Controls	
6.4 Disciplinary Process	Teleport provides audit logs and session recordings which can be used as evidence to support investigations and enforce disciplinary actions related to misuse of access or security violations.
6.7 Remote Working	Teleport enables secure, auditable access to infrastructure from any location using identity-aware policies, device trust, and encrypted connections. This allows remote workers to perform administrative tasks without exposing systems to unnecessary risk, supporting compliance with remote work security requirements.

[table continues on next page]

ISO 27001:2022 Control	Teleport Mapping
8. Technological Controls	
8.1 User Endpoint Devices	Teleport enforces device trust with access policies that evaluate endpoint attributes such as operating system, certificate presence, and software version. This is used to ensure only secure, compliant devices can access critical infrastructure, reducing endpoint-related risks.
8.2 Privileged Access Rights	Teleport binds privileged access to tightly scoped roles and attributes, ensuring all access is distributed just-in-time and time-bound. All privileged sessions are fully recorded and logged, providing accountability and enabling detailed auditing of administrative actions. Requests and approvals that require manual authorization are routed through trusted tools like Slack, PagerDuty, and more. Sensitive tasks can be configured to require a session moderator (or two session moderators) to join for approval.
8.3 Information Access Restriction	Teleport enforces strict information access restrictions through role-based access controls (RBAC), resource labels, and identity-aware policies. These controls ensure that users can only access systems, environments, or data explicitly permitted by their assigned roles, with all actions logged for accountability.
8.4 Access to Source Code	Teleport acts as a secure proxy for engineering access, securing developer and operations access to environments where source code resides, such as Git repositories or CI/CD systems. RBAC, device trust, session recording, and command logging ensures access to source code is limited to authorized personnel and is fully auditable.
8.5 Secure Authentication	Teleport strengthens authentication across infrastructure by enabling secure, modern authentication methods, including SSO integration, hardware-backed keys, biometric factors, and passwordless login via FIDO2. These capabilities ensure strong identity verification and reduce risks associated with password compromise.
8.9 Configuration Management	Teleport can control and audit access to configuration management tools like Ansible, Terraform, and Kubernetes. Enforcing RBAC, logging every configuration change session, and providing session replays helps authorized users make appropriate infrastructure modifications while ensuring all changes remain fully traceable.
8.12 Data Leakage Prevention	Teleport minimizes the risk of data leakage through short-lived access certificates, session time limits, and role-based controls that restrict access to sensitive systems. Real-time session monitoring and full audit logs provide visibility into user actions, helping detect and respond to potential data exfiltration attempts.
8.15 Logging	Teleport generates comprehensive logs of all infrastructure access events, including session start and end times, executed commands, and user identities. Logs are immutable, timestamped, and exportable to SIEM tools, ensuring complete traceability and support for compliance and forensic analysis.
8.16 Monitoring Activities	Teleport enables real-time session monitoring, including live views of user actions and the ability to terminate sessions instantly if suspicious behavior is detected. Every session is recorded and all activity is logged to increase clarity in post-event review processes.

[table continues on next page]

ISO 27001:2022 Control	Teleport Mapping
8.20 Networks Security	Teleport establishes encrypted tunnels using mutual TLS for all access, reducing the attack surface and securing traffic over public and private networks. Access policies also include device and network conditions to enforce security at the network layer.
8.21 Security of Network Services	Teleport enables secure, audited access to networked services such as SSH, Kubernetes, and databases, ensuring these services are only reachable by authenticated and authorized users via encrypted channels.
8.22 Segregation of Networks	Teleport enforces access to segmented environments (e.g., dev, staging, prod) through role-based policies and labels, ensuring users can only reach systems within their approved network zones.
8.24 Use of Cryptography	Teleport uses strong, modern cryptography including mutual TLS and short-lived X.509 certificates for secure authentication and session encryption, aligned with industry best practices.
8.25 Secure Development Life Cycle	Teleport supports secure DevOps by controlling and auditing access to development infrastructure, CI/CD pipelines, and environments. This ensures changes are made only by authorized users, with full session visibility.
8.27 Secure System Architecture and Engineering Principles	Teleport follows Zero Trust principles, enforcing least privilege, identity-bound access, and encrypted communications, which align with secure architecture best practices.
8.30 Outsourced Development	Teleport enables secure, temporary access for external developers with session recording and role-based restrictions, ensuring outsourced contributors only access the systems they're authorized to use.
8.31 Separation of Development, Test and Production Environments	Teleport enforces strict access boundaries between development, test, and production environments using role-based policies and environment-specific resource labeling.
8.32 Change Management	Teleport logs every infrastructure access and configuration change, enabling detailed tracking and review as part of formal change management processes.
8.33 Test Information	Teleport secures access to test environments and datasets by applying identity-bound access controls, ensuring test data is only used in authorized contexts and environments.
8.34 Protection of Information Systems During Audit Testing	Teleport provides access to systems under audit through scoped, monitored sessions, ensuring that testers can operate securely without compromising production environments.

[end of table]

Ready to Simplify ISO 27001:2022 Compliance?

Pass audits with flying colors and reduce the audit burden.

Use Teleport to collect, manage and govern events generated by humans, machines, workloads, and AI identities across your entire infrastructure in one place.

Get started with Teleport to meet security controls for FedRAMP, SOC 2, HIPAA, PCI, NIS2, DORA, ISO 27001:2022, and more.

Talk to an Expert →