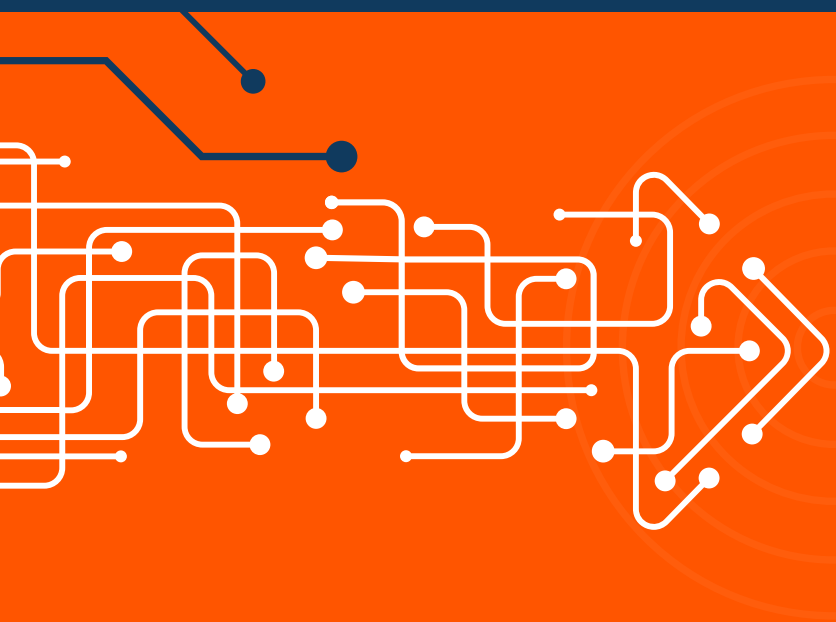
BeyondTrust

ISO/IEC 27001:2022: Using BeyondTrust to Map to the Standard



This document is informational and is intended to provide guidance on how organizations may use BeyondTrust products to meet their own obligations under ISO/IEC 27001.

BeyondTrust

TABLE OF CONTENTS

Introduction

Securing sensitive information is paramount for organizations across all industries. ISO/IEC 27001 is one of the world's best known international standards for information security management systems (ISMS), providing a systematic approach to establishing, implementing, and improving an ISMS. This standard is jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Through demonstrating compliance with ISO/IEC 27001, organizations can quickly prove the data used, owned, or stored by the organization is performed in adherence to globally-recognized best practices.

BeyondTrust maintains our own ISO/IEC 27001 certification status, employing the international standard across our core organizational functions. You can learn more about BeyondTrust certifications here: https://www.beyondtrust.com/solutions/compliance/iso-27001

About This Guide

This guide examines ISO/IEC 27001 and the updates made in the October 2022 release, referenced through this document as ISO/IEC 27001:2022. Several of the key changes made in the October 2022 update are designed to more clearly articulate the security controls, management domains, and strategies recommended by the standard.

Read this paper to learn:

- What makes ISO/IEC 27001 certification a significant achievement, and what the benefits are.
- How the certification process works and which evidence is required to achieve certification.
- How organizations can improve compliance with the standard and the security controls outlined in Annex A using BeyondTrust solutions.
- How BeyondTrust's Privileged Access Management (PAM) and Identity Security solutions help organizations satisfy or increase alignment with ISO/IEC 27001:2022 security controls.

Core Principles of ISO/IEC 27001

ISO/IEC 27001 introduced a standardized approach to information security management. Prior to its development, organizations relied on disparate security methodologies to address gaps or potential vulnerabilities across their infrastructure. This led to inconsistencies and overlap from framework to framework. In response, the International Organization for Standardization (ISO) commissioned the development of a globally-recognized standard for information security management—certifying compliant systems as optimized for risk management, cyber-resilience, and operational excellence.

Within ISO/IEC 27001 lies a set of core principles that guide organizations in establishing robust information security management systems.

These principles include:

I. Risk-based Approach: ISO/IEC 27001 advocates for a risk-based approach to information security, wherein organizations identify and prioritize threats and vulnerabilities based on their potential impact and likelihood of occurrence. By conducting risk assessments and implementing appropriate controls, organizations can effectively mitigate risks.

II. Continual Improvement: ISO/IEC 27001 emphasizes the importance of continual improvement in information security practices. Through regular monitoring, evaluation, and review, organizations can identify areas for enhancement and adapt to evolving threats and challenges.

III. Management Commitment: Leadership commitment is essential for the successful implementation of ISO/IEC 27001. Senior management must demonstrate a clear understanding of information security risks and allocate resources accordingly to support ISMS initiatives.

IV. Compliance with Legal and Regulatory Requirements: ISO/IEC 27001 encourages organizations to comply with relevant legal and regulatory requirements pertaining to information security. By staying apprised of legislative changes and industry standards, organizations can ensure adherence to applicable regulations.

V. Integration with Business Processes: Effective integration of information security measures with business processes is critical for seamless operations. ISO/IEC 27001 promotes alignment between security objectives and organizational goals, helping organizations achieve a balance between security and functionality.

Why is ISO Certification Important?

Implementing ISO/IEC 27001 offers numerous benefits for businesses, regardless of their size or industry. One of the chief benefits is to provide a structured framework for identifying, assessing, and mitigating information security risks. By conducting comprehensive risk assessments, organizations can proactively address vulnerabilities and protect their critical assets.

ISO/IEC 27001 is also designed to foster a culture of security awareness and compliance within organizations. Through the establishment of policies, procedures, and controls, employees are equipped with the necessary tools and guidelines to safeguard sensitive information. This not only reduces the likelihood of security incidents, but also enhances overall operational efficiency.

Moreover, ISO/IEC 27001 certification serves as a testament to an organization's commitment to information security. In an increasingly competitive marketplace, certification can differentiate businesses and instill confidence among stakeholders, including customers, partners, and regulatory bodies.

ISO/IEC 27001 Certification Process

Achieving ISO/IEC 27001 certification involves a series of review stages, each designed to assess an organization's compliance with the standard's requirements. While the certification process may vary depending on the certification body and organizational context, the following steps are typically involved:

Gap Analysis: The first step in pursuing ISO/IEC 27001 certification is conducting a comprehensive gap analysis to assess the organization's current state of information security management. This involves identifying areas of non-compliance and determining the scope of the ISMS implementation.

ISMS Development: Based on the findings of the gap analysis, organizations develop and implement an information security management system aligned with the requirements of ISO/IEC 27001. This entails defining policies, procedures, and controls to address identified risks and vulnerabilities.

Risk Assessment: Organizations conduct a thorough risk assessment to identify and prioritize information security risks. This involves evaluating the likelihood and potential impact of various threats and vulnerabilities, allowing organizations to implement appropriate controls to effectively mitigate risks.

Implementation of Controls: Once risks have been identified and assessed, organizations implement controls to mitigate or eliminate identified risks. These controls may include technical, procedural, or organizational measures aimed at safeguarding information assets.

Internal Audit: Prior to seeking certification, organizations conduct an internal audit to evaluate the effectiveness of their ISMS implementation. This involves reviewing documentation, procedures, and controls to ensure compliance with ISO/IEC 27001 requirements.

Certification Audit: Following the internal audit, organizations undergo a certification audit conducted by an accredited certification body. During the audit, auditors assess the organization's ISMS against the requirements of ISO/IEC 27001, verifying compliance and identifying any areas for improvement.

Certification Decision: Based on the findings of the certification audit, the accredited certification body decides regarding ISO/IEC 27001 certification. If the organization's ISMS is deemed compliant with the standard's requirements, certification is granted, and the organization receives an ISO/IEC 27001 certificate.

Annex A: Specific Security Controls

ISO/IEC 27001:2013 broadly defined the requirements for an information security management system. However, the specific control guidelines were not specified—until Annex A.

Annex A contains the specific controls organizations may wish to align with to achieve compliance with ISO/IEC 27001:2022 guidelines. Organized into four categories, Annex A serves as a roadmap for identifying, implementing, and maintaining appropriate security measures tailored to the organization's unique needs and risk profile. Alignment with Annex A not only enhances the organization's credibility and trustworthiness in the eyes of stakeholders, but also helps in achieving regulatory requirements and contractual obligations related to information security.

In the ISO 27001:2022 update, Annex controls were reorganized to better reflect current security challenges. Though core information security management system processes remain unchanged, the Annex A control set was updated to reflect more modern risks and their associated controls. Annex A of ISO 27001:2013 contained 114 controls, divided over 14 chapters; this has been restructured in the 2022 updates, which now contain 93 controls, divided over 4 chapters.

The four chapters of Annex A controls include:

- Organizational
- People
- Physical
- Technological

Using BeyondTrust to Map to Annex A Controls

In this section, we will highlight the security controls where BeyondTrust solutions can help you align with or satisfy individual control definitions, to better help you meet your requirements under ISO 27001:2022. Controls with no relationship to BeyondTrust solutions have not been included in this mapping.

M = Meets Requirement
(Can help you completely achieve or enable the control definition)

PM = Partially Meets Requirement
(Partially achieves or enables the control, or a portion of the control definition)

A = Alignment
(Can contribute to efforts correlated to the control definition)

PA = Partial Alignment
(Can partially contribute to efforts correlated to the control definition)

5. Organizational Controls									
			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	A	A	A	A	A	A	A
5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	A	A	A	A	A	A	A
5.4	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	A	A	A	A	A	A	A
5.7	Threat intelligence	Information relating to information security threats shall be collected and analyzed to produce threat intelligence.	M	A	A	A	A	A	A

			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	PM	M	M	M	PM	M	A
5.11	Return of assets	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	A	A	A	A	A	A	A
5.12	Classification of information	Control Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	A				A	A	A
5.13	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	A				A	A	A

			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
5.14	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.						A	
5.15	Access control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	PA	PA	PA	PA	PA	PA	PA
5.16	Identity management	The full life cycle of identities shall be managed.	PM	A	A	A	A	A	A
5.17	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	A	PA	PA	PA	A	PA	A

			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
5.18	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	PM	A	A	A	PM	A	A
5.19	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	A				A		
5.21	Managing information security in the information and communicat-ion technology (ICT) supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	A				A		
5.22	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	A				A		

			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	A			PA	A		
5.25	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	PM	PA	PA	PA	A	PA	PA
5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	PM				PM		
5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	A				A		
5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	A	A	A	A	A	A	A

			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.		A				A	
5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	A	A	A	A	A	A	A
5.34	Privacy and protection of personal identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.						A	
5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	A	A	A	A	A		A

			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
5.36	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	A	A	A	A	A	A	

6. People Controls									
			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
6.5	Responsibilit-ies after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	A				PM		
6.7	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	A		A	A	A	A	A

7. Physical Controls									
			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	A	A	A	A	A	A	A
7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	A				A		
7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.			PA				
7.9	Security of assets off-premises	Off-site assets shall be protected.	A	A	A	A	A	A	A
7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	A	A	A	A	A	A	

			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.		PA	PA				

8. Technological Controls									
			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
8.1	User endpoint devices	Information stored on, processed by or accessible via user end point devices shall be protected.	A	A	M	A	A	A	A
8.2	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	PM	M	M	M	M	M	M
8.3	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	PM	M	M	M	M	M	M

			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	PM	PA	PA	PA	M		
8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	M	M	M	M	M	M	A
8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	M	M	M	M	M	M	M
8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	A	A	M	A	A	A	
8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	M	A	M	A	A	A	PA

			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
8.9	Configuration management	Configurations, including security configurations, of hardware, software, services, and networks shall be established, documented, implemented, monitored and reviewed.	M	A	A	A	A	A	A
8.11	Data masking	Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.						M	
8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store, or transmit sensitive information.			A			A	
8.13	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.		A	A	A		A	

			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed.	A	M	M	M	A	M	A
8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents.	M	M	PM	M	A	PM	A
8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	A	A	A	A	A	A	
8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	A	A	M	A	A	A	A
8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	A	A	M	A	A	A	A

			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
8.20	Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.		PM				PM	
8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization's networks.		A	A	A		A	
8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	A		A	A	M		
8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.		PM		PM			A
8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	A						

			Identity Security Insights	Password Safe	Endpoint Privilege Management	Privileged Remote Access	Entitle	Remote Support	Active Directory Bridge
8.31	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	A	A	A	A	A	A	A
8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	A	A	A	A	A	A	

The BeyondTrust Platform

Ready for the Next Step?

Ready to simplify your journey toward demonstrating ISO/IEC 27001 compliance and earning or maintaining your organization's certification? **Contact our team of experts today.**

Identity Security Insights

Gain a centralized view of identities, accounts, entitlements, and privileged access across your IT estate. Detect threats resulting from compromised identities and privileged access misuse.

Password Safe

Manage privileged passwords, accounts, keys, secrets, and sessions for people and machines. Secure non-privileged employee passwords for business applications.

Endpoint Privilege Management

Remove local admin rights, enforce least privilege, prevent malware and phishing attacks, and control applications without compromising productivity.

Privileged Remote Access

Extend privileged access security best practices beyond the perimeter by granularly controlling, managing, and auditing remote privileged access for employees, vendors, developers, and cloud ops engineers. Privileged Remote Access has achieved Federal Risk and Authorization Management Program (FedRAMP®) authorization to operate (ATO) at the moderate impact level.

Entitle

Discover, manage, and automate just-in-time (JIT) access and modern identity governance and administration (IGA) across your cloud estate. Deploy in minutes, for seamless cloud permissions management that gives users the access they need, when they need it, while minimizing the attack surface and threat windows.

Remote Support

Supercharge your service desk with secure access and support for any devices, across any system, from anywhere—including Windows, macOS, Linux, Android, and iOS. Remote Support has achieved Federal Risk and Authorization Management Program (FedRAMP®) authorization to operate (ATO) at the moderate impact level.

Active Directory Bridge

Achieve streamlined identity management and access control across your hybrid environment by extending Microsoft AD authentication, SSO capabilities, and Group Policy configuration management to Unix and Linux systems.

>>> About BeyondTrust

BeyondTrust is the global cybersecurity leader protecting all paths to privilege with an identity-centric approach. We are leading the charge in transforming identity security and are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at **www.beyondtrust.com.**