RESOURCE CENTER

How password management helps companies achieve ISO 27001 certification

Get the full interactive view at https://bitwarden.com/resources/how-password-management-helps-companies-achieve-iso-27001-certification/

bitwarden

What is ISO 27001?

ISO 27001, an international standard, sets the foundation for creating, maintaining, and developing information security management systems (ISMS), including data management. Companies aiming to achieve ISO 27001 compliance or certification should consider adding ISO 27001 password management to their toolset.

The International Organization for Standardization (ISO) global group develops and publishes worldwide technical, industrial, and commercial standards. Last updated in October 2022, the ISO 27001 standard for ISMS provides a framework for data security consisting of 93 control sets. To achieve ISO 27001 certification, companies need to demonstrate compliance with all of them.

> To certify as an ISO 27001 company, you must comply with 93 control sets.

The ISO 27001 certification process consists of an audit conducted by independent certification bodies who review company data security policies and procedures, and how they are applied. The process can be a long one, but passing an ISO 27001 certification audit shows that your company has done a security risk assessment to identify potential threats, and have introduced security controls to protect against data breaches.

Table of Contents

The benefits of ISO 27001 certification and compliance

ISO 27001 certification gives organizations a competitive advantage in attracting and retaining customers because certification demonstrates robust information security controls. Certification can also attract and retain suppliers and other stakeholders concerned about how their information is managed and protected.

Even preparing for the audit process can strengthen existing ISO 27001 policies, and improve internal systems, structures, and day-to-day business processes. The risk management process can also help organizations better comply with data protection laws such as CCPA and GDPR, and avoid fines for non-compliance or loss of reputation due to an avoidable data breach.

Learn more about how your business can fortify its cybersecurity practices to pass security audits.

The ISO 27001 control sets

The 93 control sets are contained within Annex A and fall under 4 larger themes. To achieve ISO 27001 certification, companies need to demonstrate compliance with these controls. The categories are:

- Organizational controls (37 controls)
- People controls (8 controls)
- Physical controls (14 controls)
- Technological controls (34 controls)

The previous version of ISO included 114 controls divided into 14 categories. That version also included language governing secure log-on and password management systems.

The secure log-on control specified “access to systems and applications should be controlled by a secure log-on procedure when required by the Access Control Policy.” With a password manager, users benefit from adding another layer of security to logins, and having one place to help manage and integrate two-factor authentication for all websites that support it.

The password management system control stated “password management systems shall be cooperative to ensure the quality of passwords.” ISO recommends using a password manager that enables users to create strong and unique passwords and offers secure sharing capabilities for collaboration.

> **Password managers establish password strength, enforce 2FA, and use event logs to monitor user activity–all capabilities businesses must achieve to meet ISO access control, protection of PII, and endpoint protection requirements.**

The latest version of ISO 27001 addresses password management in Annex A 5.17. There are many additional Annex A requirements that can be met or supported by adopting a password manager. While not exhaustive, examples include:

- **Annex A 5.3, Segregation of duties**: Conflicting duties and conflicting areas of responsibilities shall be segregated.
- **Annex A 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.
- **Annex 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.
- **Annex A 5.16, Identity management**: The full life cycle of identities shall be managed.
- **Annex A 5.17, Authentication information**: Allocation and management of authentication information shall be controlled by a management process, including advising personnel on best practice handling of authentication information.
    - A detailed primer about this criteria lays out password recommendations with advice on managing passwords, including the ability to create secure passwords. In addition, the objective recommends organizations avoid weak, widely used, or compromised credentials.

> Given this criteria, organizations would ideally deploy a password management system that enables them to report on, and have actionable insights about, exposed, reused, weak, or potentially compromised passwords.

- **Annex 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.
- **Annex A 8.1, User endpoint devices**: Information stored on, processed by or accessible via user end point devices shall be protected.
- **Annex A 8.4, Access to source code**: Read and write access to source code, development tools and software libraries shall be appropriately managed.
- **Annex A 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.
    - This objective focuses on using multi-factor authentication for logging in securely to systems. With a password manager, users benefit from adding another layer of security to logins, and also having one place to help manage and integrate two-factor authentication (2FA) for all websites that support it. The objective also highlights that passwords should be kept confidential at all times, making a strong case for a fully encrypted password vault.

> Password management systems enable organizations to identify any items in their vaults with inactive 2FA.

- **Annex 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.
- **Annex A 8.12, Data leakage**: Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.

Did you know?

Bitwarden offers Vault Health Reports that can help foster strong cybersecurity practices and enable employees to identify accounts with weak protection.

ISO recommends using a that enables users to create strong and unique passwords and offers secure sharing capabilities for collaboration.

Achieve ISO 27001 certification with the help of a password manager

A password management system supports the numerous requirements of Annex A listed above, and with many of the requirements included in the overall control sets.

Users can keep authentication information secret, apply password best practices such as generating strong, unique passwords, and share passwords securely with a password manager that secures sensitive information with end-to-end encryption. By limiting who can see certain sensitive or critical information, password managers also help segregate duties and limit insider threats.

Organizations that use password managers establish password strength requirements, enforce two-factor authentication (2FA), and use event logs to monitor user activity — all capabilities businesses must achieve to meet ISO access control, protection of PII, and endpoint protection requirements. Most reputable password managers also facilitate SSO integration, equipping administrators with the tools they need to manage access and the authentication process. This capability helps meet the ISO secure authentication requirement.

When evaluating password managers for supporting ISO 27001 certification, organizations should evaluate if the software follows enterprise-grade security and compliance standards, such as SOC2 type 2 compliance, GDPR compliance, the Data Privacy Framework, and HIPAA. Companies should select a solution that offers end-to-end zero-knowledge encryption.

Get started with Bitwarden

Interested in leveraging the Bitwarden ISO 27001-compliant password manager to help meet ISO 27001 standards for information security management systems? Start an enterprise free trial with Bitwarden today!

Case studies:

Inventory Hive, a leading property inspection and virtual tour software platform in the UK, achieved ISO 27001 certification with Bitwarden.

Both Bitwarden Secrets Manager and Bitwarden Password Manager enable Titanom Technologies to demonstrate cybersecurity resilience and be considered for ISO 27001 certification.

> "I want to set guidelines on the password generator about how strong the password must be. That's very important right now for us to achieve the ISO 27001 certification."
>
> **Jannis Morgenstern, head of IT at Titanom Technologies**