safetica

How Safetica Helps to Comply with ISO 27001

Version: 2022-08-08

Introduction to ISO 27001

ISO/IEC 27001 is an Information Security Management Standard (**ISMS**) jointly published by the International Organization for Standardization, and the International Electrotechnical Commission. ISO 27001 lays out how businesses should manage the risks associated with information security threats, including policies, procedures, technical measures, and staff training.

Defined within the ISO 27001 standard are information security guidelines, requirements intended to protect an organization's data assets from loss or unauthorized access and recognized means of demonstrating their commitment to information security management through certification.

ISO 27001 includes a risk assessment process, organizational structure, information classification, access control mechanisms, physical and technical safeguards, information security policies, procedures, monitoring, and reporting guidelines.

What is an ISMS?

An ISMS is a holistic approach to securing the confidentiality, integrity, and availability (CIA) of corporate information assets.

Confidentiality

Confidentiality measures protect information from unauthorized access and misuse.

Integrity

Integrity measures protect information from unauthorized alteration.

Availability

Availability measures protect timely and uninterrupted access to the system.

Related Challenges and how Safetica helps to meet them

1. Information Security Policies

ISO 27001 requires you to create and implement information security policies and continually monitor whether the processing of information adheres to these policies. But how do you monitor how employees process information on the IT layer?

Safetica makes it possible to monitor user operations across an entire organization. It can recognize sensitive or confidential information and provide reports on how data is processed.

Based on Safetica's data classification, you can apply DLP policies, and thus enforce designated security policies and desired user behavior whenever users interact with sensitive or confidential information. This helps employees and contractors follow best practices or block unsecured or prohibited methods of storing and working with sensitive data.

2. Data Classification

ISMS requires you to ensure that information receives an appropriate level of protection in accordance with its importance to the organization. This means that information is handled based on its criticality and sensitivity.

Safetica allows configurable and customizable data classification. Sensitive or confidential data can be classified using Safetica's content inspection with OCR or based on its context, including user-based classification.

Security (DLP) policy configuration may follow to ensure that the respective data classification levels are managed appropriately.

The subsequent data classification protection levels are configurable as well, and allow silent logging, user notification, or enforced restriction of selected user operations.

3. (Potential) Data Leakage Notification

If you experience a security event related to information leakage, you need to be informed of the incident immediately so you can react and minimize any impact, or better yet, prevent the information from leaking at all.

In the event of an actual or attempted data security incident, Safetica's real-time email alert system notifies the appropriate personnel. It promptly reports the incident and provides sufficient detail so they can assess the impact of the situation and take follow-up actions.

Safetica also provides extensive audit records on operations performed with sensitive data. This helps to identify the depth of the breach, the sensitive documents concerned, and the individuals affected.

Using API integration, all records can also be sent to SIEM or data analytic tools, e.g., Power BI or Tableau.

4. Cryptography

ISO 27001 requires you to use secure management of cryptography keys and encryption where it is appropriate.

Safetica helps organizations manage storage encryption (Microsoft BitLocker), thus protecting data at rest. Encryption is centrally managed in the Safetica management console, with encryption keys distributed securely across secure endpoint devices, eliminating the need to share them between users.

5. Regulatory and Contractual Compliance

An important part of ISO 27001 is to adhere to all contractual and legal obligations impacting your business. This is a very tricky task for anyone who does not have the proper tools.

With Safetica, you can implement DLP policies and enforce data handling processes to ensure compliance with specific legislative, regulatory, or contractual requirements. Safetica DLP solutions also help to protect records from loss, falsification, unauthorized access, and unauthorized release. This also applies to the privacy and protection of personally identifiable information. The abovementioned features enable Safetica to be GDPR ready, PCI DSS ready, HIPAA ready, CMMC ready, and to meet contractual requirements using custom security policies.

ISO 27001 Annex A

With the implementation of Safetica you take a significant step towards complying with the following chapters of ISO 27001 Annex A:

5 Information Security Policies

6 Organization of Information Security

7 Human Resources Security

8 Asset Management

9 Access Control

10 Cryptography

12 Operations Security

13 Communication Security

14 System Acquisition, Development and Maintenance

16 Information Security Incident Management

18 Compliance

Key Use Cases

Use Case 1: Banking & Finance

Accounting services and facility management for the parent banking company needed help with implementing the security requirements set by ISO/IEC 27001.

Problem: The company handles sensitive client banking information and project documentation and needed to reinforce both their information management security system and their risk management system.

Solution: The IT department chose Safetica to handle their compliance needs, as it provides multiple tools that help companies satisfy the ISO/IEC 27001 norm requirements:

- analysis of how end-users work, with special emphasis on data handling processes
- policies set for external device management – only allow encrypted USB drives.
- data protection policies were set and fine-tuned (prohibit sensitive files from being printed, copied to unauthorized external devices, sent to external email accounts, print screen captured, or uploaded to the web).

Result: Files can only be transferred in predefined ways, and records are available for all actions. Management receives weekly summary reports on user internet activity, application use, document printing, and file lifecycles. In the event of a security incident, management is notified immediately.

Use Case 2: Transportation

Shipping-management company Franco Compania Naviera needs to fulfill ISO 27001 requirements.

Problem: The company creates and manages sensitive information that needs to be handled and protected in accordance with security standards and to provide the best service to its clients.

Solution: Safetica provides the necessary DLP functionalities to enforce security policies. All data created or moved within the organization can be classified, and is therefore protected from leakage. In case of a data security incident, IT/security managers are immediately notified, so they can investigate and respond.

Result: The company implemented the solution within 2 months without help from an external organization. It can now better monitor employee compliance with company policies, fulfills ISO 27001 requirements, and monitors sensitive information flow within the company.

Excellent Data Protection Made Easy

safetica

www.safetica.com