LAIKA

heylaika.com

ISO 27001 UNIVERSITY

Expert guidance and resources for growth-minded individuals

LAIKA

heylaika.com

TABLE OF CONTENTS

CH.01 ISO 27001 UNIVERSITY

ISO 27001 certification has risen by 450% in the past 10 years. Similar to SOC 2, ISO 27001 is another security-focused standard that enterprise buyers often require. It's internationally recognized, making it more important for businesses that cater to customers outside of the U.S.

BY MARY LISTER

Laika helps businesses comply with the thousands of requirements from regulators, auditors, standard bodies, security teams, and enterprise customers. Every industry and business model is unique. Even if compliance is entirely new to your business, Laika has the experience to help you meet your goals.

We've compiled a list of resources to help you navigate the ISO 27001 certification. To get started, jump to a chapter that answers your questions or flip through the guide in order.

ISO 27001 is the international standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It lays the groundwork and specifications for implementing an Information Security Management System (ISMS).

This ISO and IEC created ISO 27001 regulated guidelines to help businesses assess and treat threats and vulnerabilities. It tests how well your organization creates, implements, maintains and continues to improve on an ISMS that is appropriate.

A certification body needs to audit your ISMS to become ISO compliant. The assessment examines a business' established controls that align with the standards.

What is the ISO 27000 family of standards?

The ISO/IEC 27000 family is the completed set of standards that provides an international framework for information security management practices. It sets the groundwork for assessing and addressing information security risks within an organization.

In 2005, the ISO and IEC committees published the ISO series and revised the 27001 series in 2013. As part of the ISO 27000 family, the guidelines specifically focus on the implementation of the ISMS. The committees renamed and revised the series in 2019 "27001:13."

Who needs ISO 27001?

ISO 27001 is generally applicable to all businesses because it provides the framework required to secure data effectively.

Regardless of the organization's size or type, certifications specify the standards to become compliant, rather than what exactly needs to be secure.

Similar to a SOC 2 report, your business will likely need an ISO 27001 if it operates outside the US and stores sensitive information. We recommend that businesses pursue an ISO 27001 certification for regulatory reasons primarily. Our customers also come to us when a lack of certification impacts reputation or when pursuing international deals.

Why is a certification important?

Your business should leverage an ISO 27001 certification as proof of credibility with customers, partners, and regulators.

In globally competitive markets, it isn't easy for consumers to evaluate how secure their vendor practices are. A certification, like ISO 27001, makes it easier to build trust immediately. Equipping your organization with certification can help you field security questions and build a compelling story about how your business stands out right from the start.

In addition to a powerful marketing message, the **ISO 27001 certification** pairs with highly regulated General Data Protection Regulation (GDPR) requirements. Due to the overlap between the two frameworks, the ISO 27001 helps guide businesses towards stricter, required regulations internationally.

How do you implement ISO 27001?

Setting up an ISMS is the core to receiving an **ISO 27001 certification.** There are 114 controls that largely deal with four general areas:

1. Physical
2. Technical
3. Legal
4. Organizational Security

The requirements listed in the framework are the goal of controls. Controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks.

How do you maintain a certification?

The ISMS needs to be managed and maintained every year, even though ISO 27001 only needs to be audited every three years. Some controls will need yearly or quarterly reviews in order to stay in compliance. An audit is simply a snapshot in time, but your controls need to continue to operate regardless.

If your business falls out of compliance, it creates more work when the time comes to be audited again.

What does a typical ISO 27001 process look like?

Every business model is unique, therefore making the certification process different for everyone. But generally, most businesses will follow this checklist:

- → **Perform a gap analysis**
- → Classify your data
- → Build network architecture and data flow diagrams
- → Implement controls
- → Assess and mitigate risk
- → Perform a readiness assessment
- → Complete an audit

CH.02 ISMS FOR ISO 27001

ISMS stands for information security management system. It is the basis of your ISO 27001 compliance. The system organizes people, processes, and technology to protect the confidentiality, availability, and integrity of information.

Think of an ISMS as an overarching framework for auditors and the internal organization. Your ISMS should describe the purpose of each company policy, and the scope of that policy. It acts as an application letter for ISO 27001 by defining exactly what requirements your company fulfills through policies, practices, and procedures.

Confidentiality

Information and systems are kept private and safe from unauthorized access (people, processes, or entities)

This aspect of the ISMS involves tangible controls like multi-factor authentication, security tokens, and data encryption. It may also involve special training for individuals with access to restricted or classified data.

Availability

Data and systems are accessible to authorized users

Availability typically requires the maintenance and monitoring of your systems. From preventing bottlenecks and redundancy to assuring business continuity and upgrading software and hardware systems, the availability of your data should prevent data loss and disaster recovery.

Integrity

Data is complete and accurate

Finally, the integrity of your data examines trustworthiness. This aspect is vague. If you have limited access to your confidential data, the organization's protection leads to ISMS integrity.

Ultimately, you'll end up with a document specifying the governance of your systems. It should be shorter and more specific than an information security policy, for example, and focus on management and oversight. This document will establish a governance model to protect and secure your scoped systems.

CH.03 ISO 27001 VS. SOC 2

While ISO 27001 and SOC 2 frameworks have significant overlap, there are some important distinctions between the two standards.

ISO 27001 requirements are far more precise than SOC 2. Unlike SOC 2, ISO 27001 requirements are largely non-negotiable. While businesses can choose TSCs based on the business needs for SOC 2, ISO 27001 asks to complete more specific controls and processes to achieve certification. For example, there's no process to compensate for weaknesses with other controls, like leaning on RBAC for user access controls with SOC 2.

Overall, ISO 27001 is less malleable than SOC 2, a longer audit process and cycle, and requires more internal team knowledge. Let's dive into some other differences.

Customer Location

SOC 2 applies to businesses operating in North America or doing business in North America, largely within the US.

ISO 27001 is an international standard, usually required by businesses in the European Union and the UK.

Report vs. Certification

Both SOC 2 and ISO 27001 require formal audit processes, but the end results differ.

SOC 2 Report: At the completion of your SOC 2 audit, auditors will provide businesses with an in-depth report to share with customers, partners, and investors. This report includes a description of the system and controls to protect the data that is held or transferred through it. Most importantly, auditors will include a rating of the system's information security posture.

ISO 27001 Certification: In contrast, certified ISO 27001 auditors issue a 2-page certification. This includes the scope of the business' ISMS, date of issuance and expiration, and locations of the business' systems in-scope.

This certification does not include an in-depth analysis of the system like SOC 2; however, internal reports can be used to improve information security for future audits.

Scope and Timeline

Fortunately, SOC 2 and ISO 27001 walkthrough the same type of process to get compliant. From gap analysis, to control implementation, risk assessment, and audit, the two frameworks are fairly similar–and require many of the same types of controls.

SOC 2 design + implementation
3 months

ISO 27001 design + implementation
6 months

SOC 2 audit
6–12 weeks, annually

ISO 27001 audit
Internal, 3–6 weeks annually
External, 6–12 weeks every other year

Cost

ISO 27001 certification is a lengthy process that requires specific auditors to execute and issue the certification. The audit itself can be expensive, particularly with hiring two independent auditors for the internal audit and the formal certification audit. Expect ISO 27001 to be **slightly more expensive than a SOC 2 report.**

CH.04 ISO 27001 COST

The cost of an ISO 27001 certification is dependent on many factors.

What typically affects the cost of an ISO certification?

The cost of an ISO 27001 certification is variable. Unlike SOC 2, ISO 27001 is highly regulated and customized to the company. In order to get a proper estimate, your audit partner will need to know the following, among others:

1. How many employees do you have?
2. Where are offices and people located geographically?
3. What data does the application ingest?
4. Does your platform live on multiple cloud platforms?

A small business with 5 employees and 1 location might only require a few days of auditing, bringing the cost down. Whereas a larger, multi-site company could take up to 1 month of auditing. We recommend starting your compliance journey early, so your company can avoid the accrued costs associated with pushing off ISO 27001.

How much time does the ISO 27001 certification take?

The ISO 27001 audit process is broken down into two phases: an internal audit and an external formal certification audit. The internal audit, also known as a 'mini audit,' must be performed by an independent party or internal team. The formal audit can only be performed by an accredited ISO auditor. More on the audit process specifically here.

The mini-audit can take anywhere from 2 weeks to 1 month, given there is a remediation period between the mini-audit and formal audit. On the other hand, certification audits can take anywhere from 2 to 3 weeks to complete.

The certification audit is broken down into different stages; Stage 1 is normally a few days of presenting the policies and procedures to the auditor at a high level. Stage 2 occurs normally a few weeks after Stage 1 is completed where the auditor will dive into the detailed evidence to verify that the policies and procedures are being followed and comply with the ISO 27001 standard.

What are the costs associated with maintaining an ISO 27001 certification?

The pricing is dependent on each audit firm (there are only 21 audit firms in the United States!), but surveillance audits are required in year 2 and year 3 after the initial formal certification. Surveillance audits can determine whether or not the company is still operating as was originally represented in the initial certification year.

CH.05 ISO 27001 AUDIT

A certified ISO 27001 auditor needs to audit ISO 27001 to complete the certification. Here is everything you need to know about an ISO 27001 audit.

Who can perform my ISO 27001 audit?

Only an accredited ISO 27001 certification body can perform the formal audit.

According to the ANSI National Accreditation Board, ANAB, there are only 21 firms in the United States that can provide businesses with an official ISO 27001 certification. ANAB is the largest accreditation body in the western hemisphere that assesses and accredits different auditors against information security standards like ISO 27001.

What is an ISO 27001 audit?

The ISO 27001 audit process is broken down into two phases, an internal readiness assessment and an external formal audit.

Internal Readiness Assessment

First, ISO 27001 requires your company to go through a readiness assessment. This is an informal, internal review of the ISMS to check that it exists and is complete. Think of it as a mini-audit without recommendations on how to fix any problems found.

The readiness assessment audit should be performed by an independent party or an external team. Businesses commonly hire contractors to do the first audit or select a team that was not involved in the project to execute it independently.

Formal External Audit

After the internal audit is executed, an accredited ISO 27001 certified auditor performs the certification process. This involves examining the design, implementation, and operations of the ISMS.

The same auditors cannot perform the readiness assessment and the external audit. If you are considering working with consultants that provide both the mini-audit and certification, your ISO 27001 will lack integrity and quality assurance.

How long does an ISO 27001 audit take?

While the schedule of the audit is dependent on your auditing body, the certification process typically takes two weeks for investigation and two weeks to compile the final certification.

How do I best prepare for an ISO audit? What is required?

One of the biggest challenges organizations face is finding the certification body and auditor.

To become an accredited body, auditors need at least 4 years of experience in information security, go through 3 full ISMS audits, take a 5-day auditor course, and find a certification body to take a trainee program.

Due to the increased level of experience, we recommend seeking an auditor as soon as you start the ISO 27001 process. This will help you prepare your timeline appropriately and budget accordingly since the process can be costly if you fail the audit.

How much does an ISO 27001 audit cost?

Expect ISO 27001 to be slightly more expensive than a SOC 2 report.

ISO 27001 is a lengthy process requiring specific auditors to execute and issue the certification. The timing of the audit can get expensive, particularly if you have to hire two independent auditors for the internal audit and the formal certification audit.

Does ISO 27001 require an annual recertification?

ISO 27001 requires a full recertification process every 3 years.

However, auditors can perform random tests, like a pop quiz, for the following 2 years to make sure your organization maintains compliance. If your ISMS doesn't pass the quality checks, you'll need to go through the formal certification process sooner.

Thank you for reading Laika's ISO 27001 University.

If you have any questions, or need information regarding ISO 27001 or Laika, please feel free to contact us at **info@heylaika.com.**