Thoropass™

ISO 27001 Guide for Tech SMBs

thoropass.com →

Most businesses have a variety of ways to secure information—from multi-factor authentication policies to keycard-only access in an office. Whether you're just starting out or growing at breakneck speed, it can be easy to overlook security policies and practices in favor of "moving fast and breaking things." But if you want to maintain growth in the long-term, your prospects and customers need to know that their data is secure.

We know what you're thinking but the answer is NO—it doesn't need to hold up your sales cycle or cost a fortune or take a year to complete; though, it could be all of those things.

Certifications in ISO 27001 have risen by 450% in the past 10 years. If your business is overlooking the relevance and responsibility of achieving and maintaining information security, you'll almost certainly fall behind your competitors.

This guide will spell out exactly what ISO 27001 is, why businesses need it, and how to tackle getting ISO 27001 certified. So if you're a startup looking to embark on its compliance journey with ISO 27001, or an established organization looking to grow your compliance program, this guide is for you!

Table of Contents

Chapter 1

What is ISO 27001?

First things first, ISO/IEC 27001 provides specifications for creating and operating an effective Information Security Management System (ISMS). It is part of the ISO 27000 series, which provides international standards for information security management.

ISO/IEC 27001 was a joint effort developed by the International Organization for Standardization and International Electrotechnical Commission. They published the ISO series in 2005, and the first revision was in 2013, with subsequent revisions and updates. As of 2023, the most up-to-date version is "27001:2022".

Let's talk about who ISO 27001 applies to, and how to implement it.

Do I need to be ISO 27001 Certified?

This international standard is generally applicable to all organizations, regardless of size, type, or industry. That's because it simply provides the framework for securing your data effectively, instead of specifying exactly what or who needs to be secure.

To get more specific, answer these questions:

- Does your organization operate outside of the US?
- Do you transmit, store, or receive sensitive information?

If you answered yes to both, ISO 27001 is for you.

But if you're reading this, chances are you're already considering getting certified. Maybe a client has asked for a report on your information security, or the lack of certification is blocking your sales funnel. The reality is that if you're considering a SOC 2, but want to expand your customer or employee base internationally, ISO 27001 is for you. We recommend that businesses pursue an ISO 27001 certification for regulatory reasons, when it's impacting your credibility and reputation, or when you're going after deals internationally.

However, setting up an ISMS is the crux of ISO 27001. And you may be wondering...

Chapter 2

What is an ISMS?

An information security management system. It is also the basis of your ISO 27001 compliance.

The system organizes people, processes, and technology to protect confidentiality, availability, and integrity of information.

Confidentiality: 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: 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, 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 more vague, but if you have limited access to your data through confidentiality, the protection of your organization will lead to ISMS integrity.

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 like an application letter for ISO 27001 by defining exactly what requirements your company fulfilled through policies, practices, and procedures.

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.

Chapter 3

ISO 27001 Requirements

ISO 27001 defines 93 controls, which largely deal with organizational, people, technological, and physical safeguards. Keep in mind, that the requirements listed in the framework are the goal of controls. Controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks.

Below is a fairly comprehensive list of ISO 27001 requirements. The controls are categorized into 4 main themes: Organizational, People, Physical, and Technological.

Organizational Controls (37 Controls)

Organizational controls include information security policies, organization of information security, asset management practices, and access controls. In addition, this section includes supplier relationship management, incident management practices, business continuity considerations, and controls related to regulatory/statutory compliance.

People Controls (8 Controls)

The People controls include proper screening of candidates, establishing terms and conditions of employment, managing responsibilities, and providing information security awareness through education and training. Additionally, the organization establishes a disciplinary process for employees who have committed an information security breach which may lead to possible termination of employment responsibilities.

Physical Controls (14 Controls)

Physical controls are important to ensure that there is proper security of tangible assets. These controls include physical monitoring to entry points, visitor access security, asset disposal processes, and clear desk controls.

Technological Controls (34 Controls)

Technological controls are vital to the successful security of an organization's production data. This section includes controls around the security of the IT infrastructure, including authentication techniques, change management, logging/ monitoring controls, vulnerability management and data leakage techniques.

The ISO 27001 standard also has five types of attributes to categorize the controls within the four main themes to help organizations filter, sort or present controls in different views for certain audiences. Each control listed within the four themes is tagged with five attributes:

1. **Control Type**: How and when the control modifies risk in the event of an information security incident. Control types include:

   - → Preventive: Control intended to prevent an incident from occurring
   - → Detective: Control is enacted when an incident actually occurs
   - → Corrective: Control operates after the incident occurs

2. **Information Security Properties**: Characteristic of information the control intends to preserve. These properties include:
   - → Confidentiality: Information is organized in terms of who needs to have access to the sensitive data due to the nature of what the data contains.
   - → Integrity: Information is not tampered with during transmission or maintained in storage.
   - → Availability: Information is available to authorized users when needed.
3. **Cybersecurity Concepts**: These include attributes such as identify, protect, detect, respond and recover.
4. **Operational Capabilities**: This attribute relates to viewing controls related to their information security capabilities. These include Governance, Asset Management, Information Protection, Human Resource Security, Physical Security, System and Network Security, Application Security, Secure Configuration, Identity and Access Management, Threat and Vulnerability Management, Continuity, Supplier Relationships Security, Legal and Compliance, Information Security Event Management, and Information Security Assurance.
5. **Security Domains**: There are four domains that controls could be attributed to, which include:
   - → Governance and Ecosystem: This domain includes Information System Security Governance & Risk Management, as well as Ecosystem Cybersecurity Management.
   - → Protection: This domain includes IT Security Architecture and Physical and Environmental Security.
   - → Defence: This domain includes Detection, and Computer Security Incident Management.
   - → Resilience: This includes Continuity of Operations and Crisis Management.

Chapter 4

Implementing ISO 27001

When you're looking at implementing any new compliance framework, you'll need to consider the scope of the controls. Simply, think about which sectors of your organization will need to comply with ISO 27001 and implement an ISMS.

The scope is less of a consideration when you're leading a smaller organization or a start-up; you can consider almost all employees within the scope.

Gap Analysis

If your company has been operating for a couple of years, it's likely that you already have some best practices in place. For instance, having a formal hiring process and privacy policy is fairly common. Before diving into each specific control, you'll need to understand where the biggest gaps are and how to prioritize them.

Your compliance team will need to perform a gap analysis against the ISO 27001 framework as the first step in your implementation process. This will help with the initial organization moving into the next step.

Data Classification

Once the team understands the gaps in your current systems, they can move onto data classification. Most data classification falls into four categories: Classified/restricted, confidential, internal, and public. You should define each category and which types of data fall into each.

Public: Data that may be freely disclosed to the public

- → Marketing materials
- → Contact information
- → Price list

Internal only: Not meant for public disclosure

- → Battlecards
- → Sales playbooks
- → Organization charts

Confidential: Sensitive data that, if compromised, could negatively affect operations

- → Contact with vendors
- → Employee review

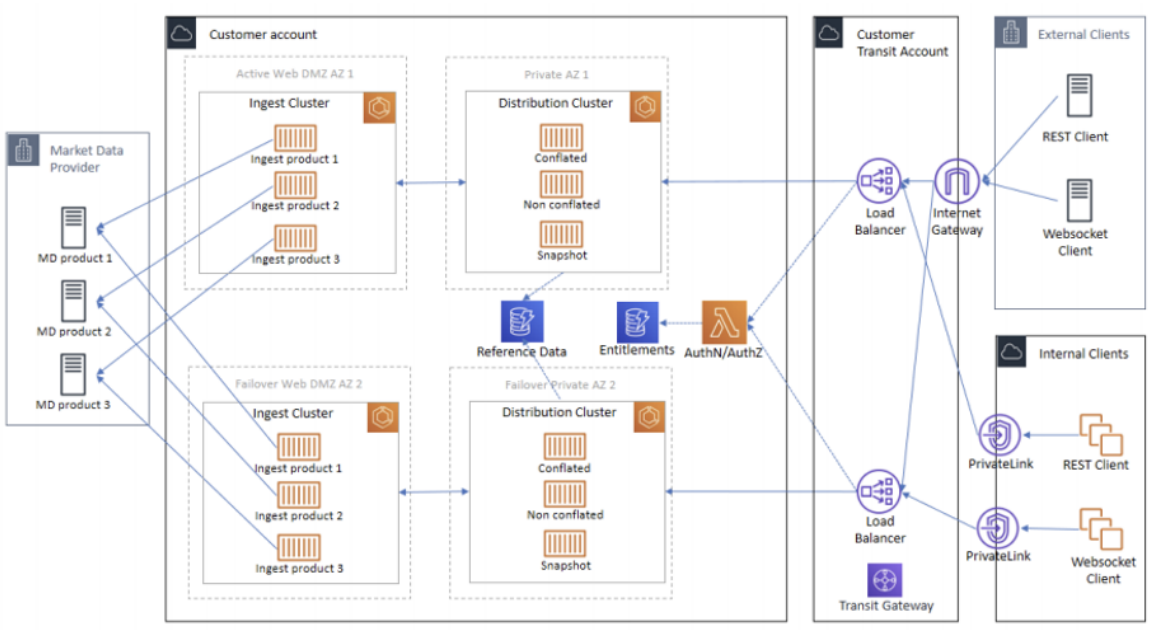
Restricted: Highly sensitive corporate data that, if compromised, could put the organization at financial or legal risk

- → Intellectual property (IP)
- → Credit card information
- → Social security numbers
- → Protected Health Information (PHI)

This step helps define controls that need to be incorporated based on the data you collect, store, and share.

Network Architecture and Data Flow Diagrams

After understanding the data that lives in your ecosystem, you'll want to know how it flows through the organization and who has access to it. Your compliance team will also be able to identify opportunities for the data to be compromised internally or externally through flow diagrams.

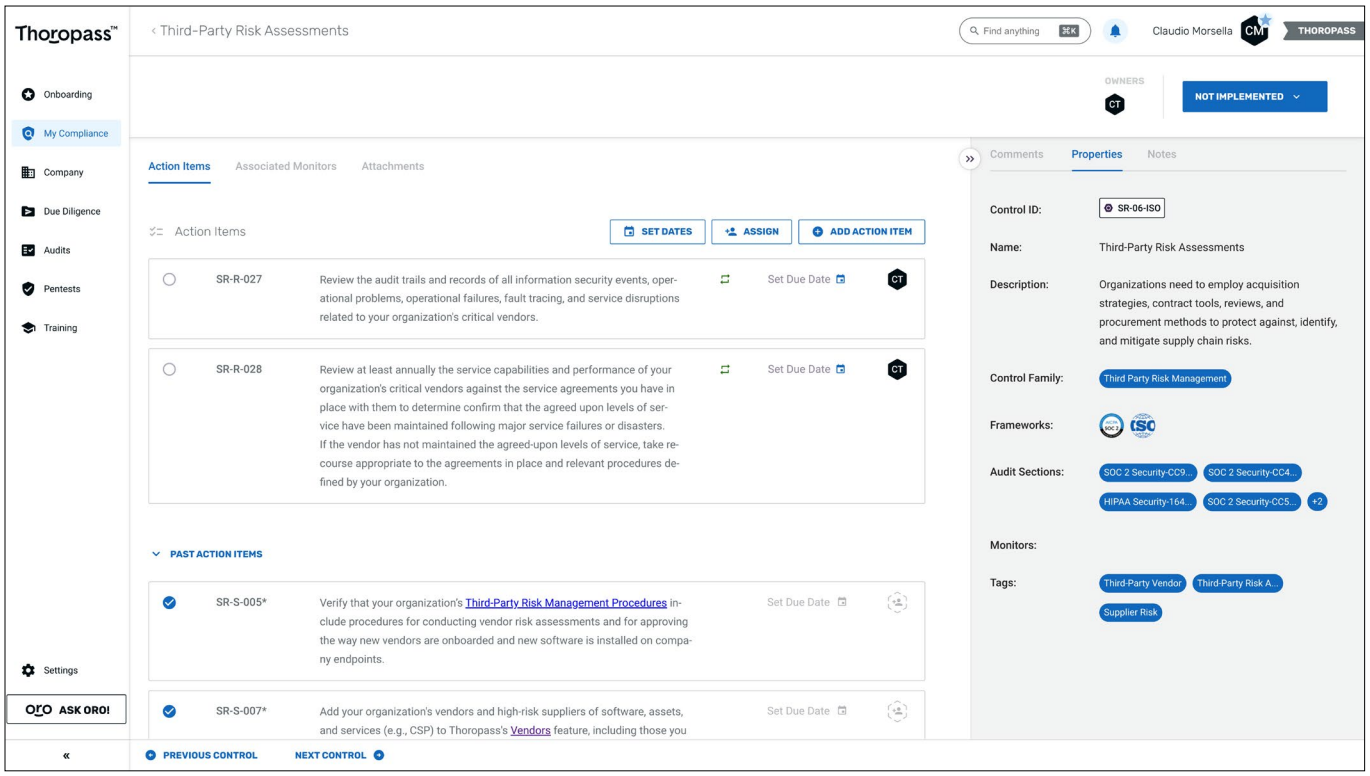


AWS provides their diagrams to the public here.

This allows you to start putting together your risk profile fastest and most efficiently by seeing what data is important, where it is stored, and how it's used. You can use any flow diagram tool to complete this step; we recommend Lucidchart.

If you have yet to establish an internal compliance team, check out Thoropass's Partner Ecosystem for the support you need!

Below is an example from Thoropass on how control implementation can be organized and tracked when using software that incorporates smart automation and key integrations.



ISO 27001 documentation can be the biggest lift of implementation. Because the framework prescribes more procedural documents like policies, the emphasis on writing those policies takes a significant amount of time. Similarly, setting up infrastructure for regularly scheduled reviews, like access control, also requires time and commitment from participants.

To avoid writing these policies on your own, from scratch, you can partner with a consultant or service, like Thoropass, that offers templated policies.

Risk Assessment

ISO 27001 requires a risk assessment, which should be executed by a qualified and knowledgeable compliance team. The risk assessment examines future plans and anticipated business growth to understand upcoming risk. That could include geographic challenges, data loss prevention, re-evaluation of scoped programs, and any concerns outside of the ISO 27001 framework controls. The team executes risk assessments after control implementation but before the audits. Based on your findings, the team can decide if the risk is acceptable or needs further control implementation to mitigate.

Risk Mitigation Controls

Implementing more controls is, as above, dependent on the amount of risk your organization is comfortable operating with. This step could be skipped if the risk assessment was found to be acceptable.

Statement of Applicability

The final step to completing the risk assessment for ISO 27001 is documenting your Statement of Applicability. This is your opportunity to identify all of the applicable controls from the ISO 27001 standard and provide justification for including them in your security program and how those controls help mitigate risks you've already identified within your risk assessment. You will also need to provide justification for excluding controls that are not applicable to your organization as well.

Monitoring and Maintaining your ISMS

Some of your controls will need periodic execution, like quarterly access reviews or logging monitoring systems. Tech SMBs should always leverage existing functionality provided by cloud services providers to prevent extra headaches.

Keep in mind that an audit is simply a snapshot in time, but your controls need to continue to operate between annual audits. Otherwise, it's likely that your business will fall out of compliance, and create more work when the time comes to be audited again.

Chapter 5

ISO 27001 Certification Process

Getting ISO 27001 certified is more difficult than SOC 2 certification, largely because there are fewer auditors and the process takes longer. The initial audit process is two steps:

Step 1: Internal Audit

First, ISO 27001 requires your company to go through an internal audit, which is really a mini-audit without the recommendations on how to fix any problems they find. It's an informal, internal review of the ISMS to check that it exists and is complete. This audit should be performed by an independent party, or an external team. We've seen contractors hired to do the first audit, other companies select a team that was not involved in the project to execute it independently. At the end of this internal audit, you'll receive a spreadsheet with a checklist with all the controls and whether they have been implemented by your team.

Step 2: Certification Audit

After your ISMS is deemed ready, an ISO 27001 certified auditor will need to perform a formal compliance audit. This involves examining ISMS to determine that it was properly designed, implemented, and is currently operating. While the schedule of the audit is dependent on your auditing body, in our experience this audit typically takes about two weeks for investigation. After that stage, your auditors should take another two weeks to compile a final report. Keep in mind that you can fail ISO 27001, unlike SOC 2. If auditors find that your information security has major issues, they will require your organization to go back and fix them to be reviewed again before handing over a certification. This process can be costly; it's important for your budget to get it right the first time around.

Chapter 6

Staying ISO 27001 Compliant

After your initial ISO 27001 certification, it can sometimes get a little more complicated to stay compliant.

For the following two years, your organization will be required to undergo a surveillance audit, where your ISMS and mandatory ISO 27001 controls are reviewed, as well as a sample of your more technical controls are audited to ensure that they are still operating based on your initial certification. In the third year of certification, your organization will go through the full audit process again.

Chapter 7

ISO 27001: Tips from Thoropass Experts

Compliance with any framework has its challenges, and ISO 27001 is no different. Because these requirements are meant to build information security into the foundational operations of a business, it can be a big lift. Here are some of the most common challenges our team has seen implementing and maintaining ISO 27001 and how to manage them.

Lack of Certified Auditors

The main challenge we see with our clients is finding a certification body and auditors. We recommend seeking an auditor as soon as you start the ISO 27001 process. You can prepare your timeline appropriately and more accurately communicate the deadline for certification clients, employees, and investors. With Thoropass, you can opt to take advantage of the Seamless Audit Experience to save yourself the hassle of finding a certified auditor on your own.

Annual Internal Audit

For most businesses, an annual internal audit can be a difficult process. When your business is small enough, it's hard to have an independent team that is knowledgeable in ISO 27001 compliance execute the exercise. Often, teams will look for external consultants to perform the internal audit, incurring an otherwise avoidable cost.

Structure-Heavy Requirements

Unlike other certifications, ISO 27001 requires organizations to build an ISMS and author structured documents. These additional documents may not be inherently valuable to your business; compliance teams often struggle to find ways to make those documents useful instead of simply an exercise to receive a participation ribbon. For example, your ISMS provides auditors with a lens to view your ISO 27001 security posture. But to anyone other than auditors, it's not a very useful document. You'll need to spend time developing and editing it nonetheless.

Asset Inventory

Our experts always recommend that our clients have a thorough asset inventory to speed up the audit process. Building an asset inventory involves classifying your assets, e.g. data warehouses, cloud environments, databases, and any components of an application. Once you understand where all your assets are and how data is stored or transferred through them, you'll be able to better design a compliance program to protect your assets.

Note: your internal audit cannot be performed by the same party as your external audit. These two steps need to be completely independent of each other. In fact, Thoropass offers an internal audit that can be added on to the core subscription. Reach out to an expert if you'd like to learn more.

We're compliance experts, so you don't have to be.

Thoropass™

Get in touch →