ISO 27001 Checklist

Easy To Follow Implementation Guide

strongdm

Table of Contents

ISO 27001 Checklist Overview

The International Standards Organization (ISO) 27001 standard is one of 12 information security standards that are increasingly relevant in a world where companies need to convey their commitment to keeping the intellectual property, sensitive data, and personal information of customers safe.

Certification happens slowly, over the course of multiple ISO 27001 phases. The first step is deciding whether a company stands to benefit most from SOC 2 versus ISO 27001 certification, prepare for the costs of certification, and get an overview of the process when carrying out your ISO 27001 compliance checklist.

However, implementing ISO 27001 certification with or without an ISO 27001 checklist can be an overwhelming process with multiple moving parts. And after downloading the standards, companies can still be at a loss for how to implement them and pass an audit.

So why is an ISO 27001 checklist important? It directs information security teams to practical information about what they'll need to prepare for certification, step by step. An ISO 27001 audit checklist streamlines the certification process and ensures that teams won't overlook something over the course of four months (for small teams) to over a year (for large companies).

Finally, an ISO 27001 compliance checklist gives you a bird's eye view of the recommended steps so you can allocate resources accordingly from the very beginning, saving time and energy.

ISO 27001 Checklist

- [ ] Assign Roles
- [ ] Conduct A Gap Analysis
- [ ] Develop And Document The Parts Of Your ISMS Required For Certification
- [ ] Conduct An Internal Risk Assessment
- [ ] Write A Statement Of Applicability (SoA)
- [ ] Implement Your Controls
- [ ] Train The Internal Team On Your ISMS And Security Controls
- [ ] Conduct An Internal Audit
- [ ] Have An Accredited ISO 27001 Lead Auditor Conduct The ISO 27001 Certification Audit
- [ ] Plan For Maintaining Certification

ISO 27001 Checklist: 10 Steps To Compliance

This ISO 27001 controls checklist offers a framework, but the certification process looks different for every company and their distinct tech stacks. Some differences in the certification process emerge based on a company's size, existing documentation, and your information security management system (ISMS).

1. Assign Roles

Some companies choose an in-house implementation lead and have employees create security documentation and conduct internal audits. Others prefer an outside consultant or contractors. The first step on your ISO 27001 checklist is to make this crucial decision based on your employees' expertise and your capacity to divert teams from existing priorities for lengthy, in-depth security work.

2. Conduct A Gap Analysis

A gap analysis looks at your existing ISMS and documentation and compares them to the ISO 27001 standards, and you can get a better sense of what to look for, if conducting your own, with an ISO 27001 gap analysis checklist.

You'll walk away from the analysis with compliance gaps that should define your preparation process and a timeline for how long it will take to reach compliance. Without this personalized roadmap, companies can spend time and money on projects that aren't directly tied to certification.

3. Develop And Document The Parts Of Your ISMS Required For Certification

Companies undergoing certification for the first time will need to set up parts of their ISMS and identify the areas requiring protection. Your ISMS will consist of all the internal ISO 27001 policies and procedures in place for cybersecurity. It consists of people, processes, and technology, so it necessitates looking at how information is accessed, when, and by whom.

You'll find all locations where data is stored, document how it is accessed, and make policies to protect it at these touchpoints (hint: you can find ISO 27001 templates for much of the work you'll need to present at your audit). Consider both physical and digital data in this step.

4. Conduct An Internal Risk Assessment

Now that you know all about your data, it's time to document the known risks to that data. An ISO 27001 asset management checklist, ISO 27001 network security checklist, ISO 27001 firewall security audit checklist, or an ISO 27001 risk assessment checklist can help you identify and document these risks.

How likely are they to occur? How severe would the impact be if they occurred? How will you decide? The process starts with determining how you'll identify and rate risks. A risk matrix can help you prioritize high likelihood and high impact risks to sort them accordingly. For each risk, develop a response plan and assign

team members accountable for following up. For external data centers, an ISO 27001 data center audit checklist can help you document quality control and security procedures.

5. Write A Statement Of Applicability (SoA)

It's time to dig into the ISO 27001 guidelines. In Annex A, you'll find a list of 114 possible controls. Select those that address the risks you identified in your risk assessment. Then write a statement about which controls you will apply. You will need this document for the audit process.

6. Implement Your Controls

Now that you've compared your policies and systems to the ISO 27001 controls and applied controls to your own ISMS, it's time for your workplace's systems to reflect what you documented.

You may need to update software, procedures, or policies regarding how people handle data. For example, if you have verified that your organization will use cryptography to protect information confidentiality, you'll need to add that layer to your stack.

7. Train The Internal Team On Your ISMS And Security Controls

It's time to dig into the ISO 27001 guidelines. In Annex A, you'll find a list of 114 possible controls. Select those that address the risks you identified in your risk assessment. Then write a statement about which controls you will apply. You will need this document for the audit process.

8. Conduct An Internal Audit

An internal audit prepares you for the official audit and tests your new systems. Are your controls working? This can be conducted by an internal team that was not a part of setting up and documenting your ISMS, or an independent external reviewer.

An internal audit lets you know and gives you the chance to make changes before the official audit. To get started, try using an ISO 27001 self-assessment checklist or an ISO 27001 internal audit checklist.

9. Have An Accredited ISO 27001 Lead Auditor Conduct The ISO 27001 Certification Audit

You'll need an accredited ISO 27001 auditor from a recognized accreditation body to conduct a two-step audit: first, they'll review your documentation and controls. Get a handle on this portion of the audit ahead of time by working through an ISO 27001 stage 1 audit checklist.

Next, the auditor will perform a site audit. They'll perform tests on your controls to ensure they're being followed. You guessed it: you can get ahead of this step too, with an ISO 27001 stage 2 audit checklist. You'll get a list of major and minor nonconformities for each step, and once major nonconformities are addressed, you'll be issued ISO 27001 certification.

10. Plan For Maintaining Certification

ISO 27001 certification lasts three years, but you'll conduct risk assessments and surveillance audits each year while preparing new documentation for your renewal audit in the third year. In addition to updating your policies and systems and managing your ISMS, there's ongoing employee training to schedule annually.

Overall, the steps you'll need to fulfill ISO 27001 guidelines can be broken down into multiple smaller checklists. Depending on the needs of your organization, make use of resources like an ISO 27001 Annex A checklist, ISO 27001 evidence checklist, ISO 27001 gap analysis checklist, or ISO 27001 surveillance audit checklist.

ISO 27001 Implementation Tips

ISO 27001 is a detailed standard, and it's impossible to be familiar with your industry's best practices beforehand. However, some simple tips can get you started on your ISO 27001 checklist.

Study Up On ISO 27001 And ISO 27002 Standards

The ISO 27002 standards have additional information on each Annex A control you can use to write an expert SoA (step 5 on your ISO 27001 checklist).

Prepare Ahead Of Time

Preparation for the official audit is a large chunk of the certification process. Even with all that prep work, audits can leave your team rushing to find more information to support their processes at the 11th hour.

Get input on your documentation early. Record and track meetings, and implement a project management system that identifies who will do which tasks and when tasks will be completed. Your project management team can take control of working through your ISO 27001 checklist, making sure everything is in order for a complete ISO 27001 implementation roadmap.

Talk To Reviewers

During audits, you'll get information on nonconformities that will later appear in your written report. But, diving into the details in person can help you interpret that report. Get as much clarity and alignment as possible, so you're confident you know how to make the changes that will lead to better results next time.

Find Experts

By the end of the process, many employees feel they've become experts in the process. But, at the onset and along the way, it can be challenging to extrapolate your industry's and organization's needs pertaining to certification. Guessing means time and energy spent on tasks that won't lead to certification. So whether it's a consultant, hiring the talent to lead certification, or tapping your certification body, choose clarity over making assumptions.

How Can StrongDM Help You With ISO 27001 Certification?

First, stay on top of preparing for an audit by working through the steps of this ISO 27001 checklist. Then, look to StrongDM to help design and implement better security and system audits needed to get and stay ISO 27001-compliant.

We manage and audit access to your databases, servers, clusters, and web applications to cover, manage, and document all those points of contact you identified in your risk assessment. We can help you determine the kinds of controls needed and help you implement them in the most efficient way possible.

If you want to learn more about how StrongDM can help you simplify ISO 27001 Certification, make sure to check our **ISO 27001 Compliance Solution Guide** or **schedule a no-BS demo** to see it all in action.

strongdm

strongDM's infrastructure access platform gives every business secure access controls in a way folks love to use. Trusted by the Fortune 500 to fast-growing businesses like Peloton, SoFi, Chime, Yext, and Better, strongDM gives businesses the control and visibility they need at the speed they want with one platform that works for every environment. strongDM is intentionally distributed. Head to **www.strongdm.com** to learn more.