secureframe

The Ultimate Guide to ISO 27001

Table of Contents

An introduction to ISO 27001

ISO 27001 is one of the most respected information security standards around the globe. It's a rigorous standard that ensures organizations have best-in-class data security customers can trust.

For high-growth companies, certification is also the price of admission for moving upmarket and expanding into new geographies. Customers expect the partners they work with to be ISO 27001 certified, and deals are lost without it.

You understand the importance of protecting company and customer data from costly breaches. You wouldn't be reading this if you didn't.

This guide breaks down the fundamentals of the ISO 27001 standard. It explains the basic requirements for a compliant Information Security Management System (ISMS), outlines ISO 27001 control requirements, details the audit process, and includes tips and resources to help you achieve certification.

Part I: Understanding ISO 27001

ISO 27001 is a security framework created by the International Organization for Standardization. It assesses a company's ability to keep its data safe.

To achieve certification, companies must complete an audit to verify that they meet ISO 27001's rigorous standards.

Pursuing ISO 27001 certification holds a lot of benefits for growing businesses. Aside from keeping your data safe from a breach, it can:

- Build trust with customers
- Inspire confidence in shareholders and investors
- Improve business processes and policies
- Give you a powerful competitive advantage

What is the ISO 27001 standard?

When it comes to IT security, ISO 27001 certification is one of the most respected standards internationally.

The ISO 27001 standard was established in 2005, then revised in 2013 and 2017 through a partnership with the International Electrotechnical Commission (IEC). The framework is designed to evaluate whether an organization's information security management system (ISMS) can protect sensitive data.

An ISMS is more than just the hardware and software you use to keep information safe — it's a set of rules that govern how you use information. How you store and retrieve it, how you assess and treat risk, and how you continuously improve data security.

If an independent auditor confirms that your company's ISMS meets the standards, you are granted ISO 27001 certification.

ISO 27001 vs 27002

Both ISO 27001 and 27002 are information security standards created by the International Organization for Standardization. Both explain how to create a secure ISMS. And both discuss the controls organizations can use to protect their data.

So what's the difference between them?

ISO 27001 is what's known as a management standard. Management standards explain how to run a system — in the case of ISO 27001, an information security management system.

ISO 27002 is not a management standard. It's a set of guidelines and security techniques. While you can undergo an audit to become ISO 27001 certified, you can't get an ISO 27002 certification.

There's also a big difference in the level of detail each standard goes into. For example, the ISO 27001 standard explains how to build an ISMS: the responsibilities of company management, how to set and measure objectives, how to do an internal audit, and how to design controls.

But it doesn't get into the nitty-gritty details of every single control. ISO 27002 does. It covers the goal of each control, how it works, and what companies can do to implement it successfully.

	What is it?	**When should you use it?**
ISO 27001	A management standard that defines how to build an information security management system	When you need to scope, design, and build a compliant ISMS
ISO 27002	A set of guidelines and techniques for implementing security controls	When you're ready to implement specific security controls to safeguard your ISMS

ISO 27001 vs SOC 2

A lot of fast-growing companies face the ISO 27001 vs SOC 2 debate when deciding which type of compliance to pursue. And it's a tough decision to make — partly because the two frameworks are so similar.

Both frameworks:

- Prove to clients that you can be trusted with their data
- Cover foundational security principles like data integrity, availability, and confidentiality
- Require an independent audit by a certified third party
- Need significant time, effort, and money to achieve

Are you better off pursuing ISO 27001 certification or a SOC 2 report? Which holds more prestige with your customers? Is one more difficult to get than the other?
Use this SOC 2 vs ISO 27001 comparison to understand the key differences between the two frameworks.

	SOC 2	ISO 27001
Overview	Service Organization Controls on Trust Services Principles and Criteria for Security	International Organization for Standardization/IEC 27001
Accreditation body	AICPA	ANSI-ASQ National Accreditation Board [ANAB]
Target Market	United States	International
Core Requirements	Trust Service Criteria: Security*, Availability, Confidentiality, Processing Integrity, and Privacy * Security is the only required criteria	Clauses 4.1-10.2 of the framework, including ISMS scope, Statement of Applicability, Risk Management, etc.
Audit Result	SOC 2 attestation report, typically made available only under NDA. Reports don't expire, but customers typically require a new SOC 2 every year.	ISO report, including a l-page certification that can be made public. Surveillance audits in years 2 and 3, with recertification required after 3 years.
Timeline	1-4 moths for Type | report; 6-12 months for Type II report.	Approximately 10-12 months
Cost	Varies by size and complexity of organization; typically $10-60k.	Varies by size and complexity of 'organization; typically $10-25k

Who needs ISO 27001 certification?

Any company handling sensitive data should seriously consider pursuing ISO 27001 certification. This includes customer data, employee data, or internal proprietary data.

ISO 27001 certification gives customers, internal stakeholders, and investors assurance that you have a robust security management system in place.

While ISO 27001 is popular worldwide, it's most commonly requested by international customers (especially those in Europe). If your company has European customers or is planning on expanding into the global market, ISO 27001 certification is a must.

Protect customer data

Comply with laws and regulations

Improve overall security posture and business process

Avoid costly data breaches

Send positive signals to investors & shareholders

Enhance brand reputation & win new customers

Why is ISO 27001 important?

ISO 27001 certification requires a significant investment. And not just financial: you'll need to dedicate a lot of time and internal resources to preparing for and completing certification.

But even for small companies with few resources to spare, pursuing certification can pay off in a big way. Here are some advantages of being ISO 27001 certified:

- Gain a competitive go-to-market advantage, particularly internationally
- Win deals against non-ISO 27001 compliant competitors
- Speed up the sales cycle by removing security and compliance as an objection
- Sell upmarket by gaining the trust of larger enterprises
- Strengthen customer trust by proving that your service is secure.
- Get an expert third-party opinion on your security controls and policies
- Build a company culture of security and compliance
- Improve investor and partner confidence

Part II: Getting ISO 27001 Certified

ISO 27001 is a rigorous standard, and it can be intimidating to tackle if you're pursuing certification for the first time.

Which policies and controls will you need? How do you know if you're ready for an audit? Understanding the ISO 27001 certification process can help you better prepare and remove a lot of unnecessary stress.

The ISO 27001 certification process

Months 1-4: Audit preparation

To achieve ISO 27001 certification, you'll need to undergo a series of audits. Here's what you can expect as you prepare for your certification.

Step 1: Create a project plan

Who within your organization will oversee the certification process, set expectations, and manage milestones? How will you get buy-in from company leadership?

Build an ISO 27001 team to manage each step of the preparation process, coordinate with the auditor, and oversee maintenance.

Step 2: Define the scope of your ISMS

Each business is unique and houses different types of data. Before building your ISMS, you'll need to determine exactly what kind of information you need to protect.

For some companies, the scope of their ISMS includes their entire organization. For others, it only includes a specific department or system.

Your team should discuss what you want represented in the scope statement of your ISO 27001 certificate. Start by asking yourself: "What services, products, or platforms do our customers expect to see as part of our ISO 27001 certificate?"

Step 3: Perform a risk assessment and gap analysis

A formal risk assessment is required for ISO 27001 compliance. That means the data, analysis, and results of your risk assessment must be documented.

To start, consider your company's baseline for security. What legal, regulatory, or contractual obligations are you being held to? What do your customers expect from you?

Many startups that don't have a dedicated compliance team choose to hire an ISO consultant to help with their gap analysis and remediation plan. Although it's an added cost (typically in the $30-40k range), a consultant who has experience working with companies like yours can offer expert guidance and help you meet compliance requirements.

Step 4: Design and implement policies and controls

Now that you've identified risks, you'll need to decide how your organization will respond. Which risks are you willing to tolerate, and which do you need to address?

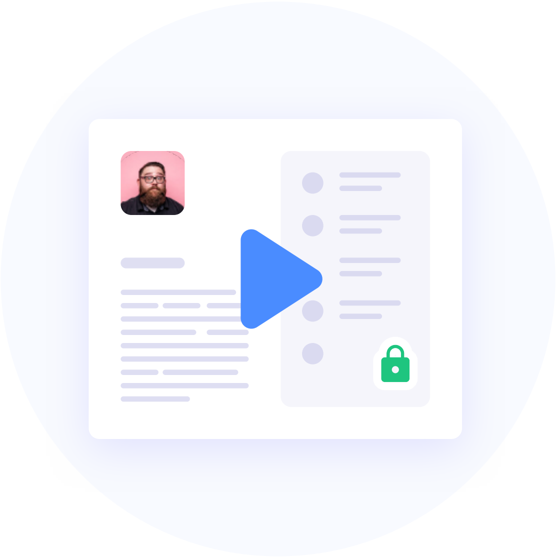
Your auditor will want to review the decisions you've made about each identified risk. You'll also need to produce a statement of applicability and a risk treatment plan as part of your audit evidence.

The Statement of Applicability summarizes and explains which ISO 27001 controls and policies are relevant to your organization. This document is one of the first things your external auditor will review.

Your risk treatment plan records how your organization will respond to the threats you identified during your risk assessment process. The ISO 27001 standard outlines four possible actions:

- **Modify** the risk by establishing controls that reduce the likelihood it will occur
- **Avoid** the risk by preventing the circumstances where it could occur
- **Share** the risk with a third party (i.e., outsource security efforts to another company, buy insurance, etc.)
- **Accept** the risk because the cost of addressing it is greater than the potential damage

Next, you'll build policies and controls in response to identified risks. Your policies should establish and reinforce security best practices, like requiring employees use multi-factor authentication and lock devices whenever they leave their workstations.



Step 5: Complete employee training

ISO 27001 requires all employees to be trained about information security. Everyone in your organization needs to understand the importance of data security — and their role in achieving and maintaining compliance.

Step 6: Document and collect evidence

To get ISO 27001 certified, you'll need to prove two things to your auditor. First, that you've established effective security policies and controls. And second, that they're functioning as required by the ISO 27001 standard.

Gathering and organizing all this evidence can be extremely tedious and time-consuming. Compliance automation software can eliminate hundreds of hours of busy work by collecting this evidence for you.

Months 5-12: Certification audits

You've built your ISMS. You've completed a gap assessment and implemented controls. You've trained your staff. And you've diligently documented every step.

Now, you're ready to begin the audit process.

Step 7: Complete an ISO 27001 certification audit

A formal ISO 27001 audit happens in stages:

Stage 1: ISMS Design review

At this stage, your auditor will review ISMS documentation to make sure all of the required policies and procedures are in place and properly designed. They will make sure your documentation is compliant with the requirements listed in clauses 4-10 of the ISO 27001 standard document. They will also point out any nonconformities or opportunities to improve your ISMS.

Once you've implemented any suggested changes, you're ready for your Stage 2 audit.

Stage 2: Certification audit

This is where your auditor will complete a detailed assessment to determine whether your organization satisfies ISO 27001 standards. They will review your business processes and controls to ensure compliance with ISMS and Annex A requirements.

Once Stage 1 and Stage 2 are complete, you're issued an ISO 27001 certification that's valid for three years.

Surveillance audits

Within your three-year certification period, you'll need to conduct ongoing audits. These audits ensure your ISO 27001 compliance program is still effective and actively being maintained.

Surveillance audits ensure organizations are managing their ISMS and Annex A controls properly. Surveillance auditors will also check to make sure any nonconformities or exceptions noted during the certification audit have been addressed, and that there's a remediation plan in place for any new nonconformities that have been identified.

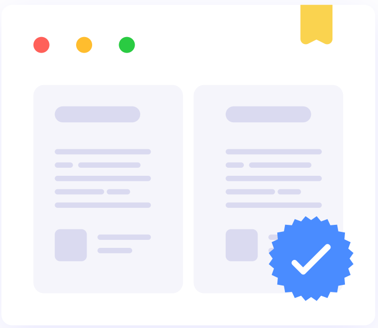
Recertification audit

During the last year of the three-year ISO certification term, your organization can undergo a recertification audit.

Similar to a Stage 2 audit, the auditor will complete a detailed assessment to determine whether your organization still meets ISO 27001 requirements. They'll examine process/control design and operating effectiveness.

After the recertification audit, your ISO 27001 certification is valid for another three years.

The ISO 27001 certification audit process

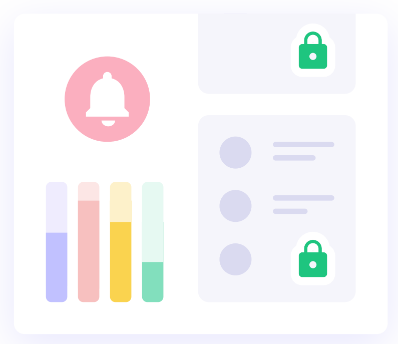


Stage 1: ISMS Design Review

Review ISMS documentation to make sure policies and procedures are properly designed.

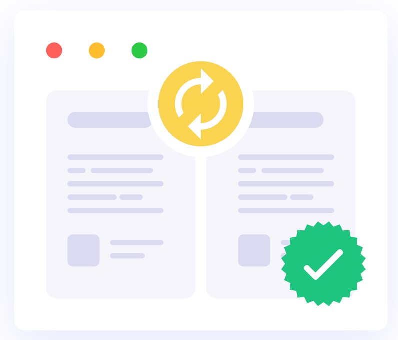
Stage 2: Certification audit

Review business processes & controls for compliance with ISMS and Annex A requirements.



Surveillance audits

Ensure your ISO 27001 compliance program is still effective and being maintained.



Recertification audit

At the end of the 3-year certification term, a recertification audit assesses ISMS and Annex A controls for compliance. Recertification is valid for another 3 years.

Step 8: Maintain compliance

ISO 27001 is all about continuous improvement, so you'll need to keep reviewing your ISMS to make sure it's operating effectively. As your business evolves and new threats emerge, you'll need to watch for opportunities to improve existing processes and controls.

The ISO 27001 standard requires periodic internal audits as part of this ongoing monitoring. Internal auditors examine processes and policies to look for potential weaknesses and areas of improvement before an external audit.

How much does ISO 27001 certification cost?

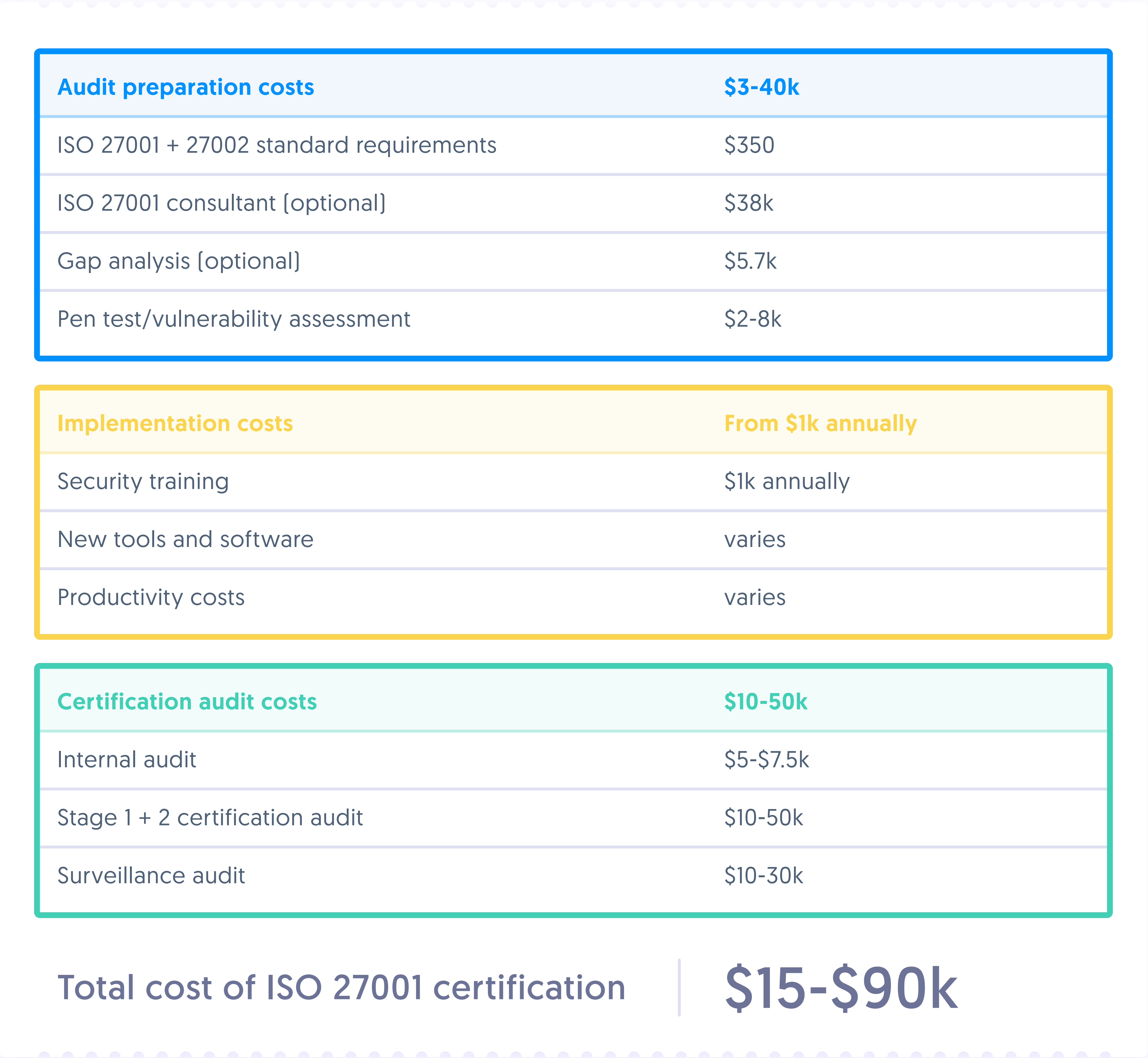
The cost of an ISO 27001 certification varies significantly depending on:

- The size of your organization
- Number of office locations
- Type of data your ISMS houses
- Internal expertise vs. hiring consultants

The smaller and less complex your organization, the less you're likely to pay. That said, it can be helpful to have specific numbers in mind when estimating your own ISO 27001 compliance costs.

On average, companies can expect to pay:

- Up to $40,000 during the audit preparation process
- $15,000+ for the certification audit
- $10,000 per year for maintenance and surveillance audits



Audit preparation costs	$3-40k
ISO 27001 + 27002 standard requirements	$350
ISO 27001 consultant (optional)	$38k
Gap analysis (optional)	$5.7k
Pen test/vulnerability assessment	$2-8k

Implementation costs	From $1k annually
Security training	$1k annually
New tools and software	varies
Productivity costs	varies

Certification audit costs	$10-50k
Internal audit	$5-$7.5k
Stage 1 + 2 certification audit	$10-50k
Surveillance audit	$10-30k

Total cost of ISO 27001 certification | $15-$90k

There are ways to reduce the cost of ISO 27001 certification. If you're also pursuing a SOC 2 report, your auditing firm may give you a discount for completing both certifications at once.

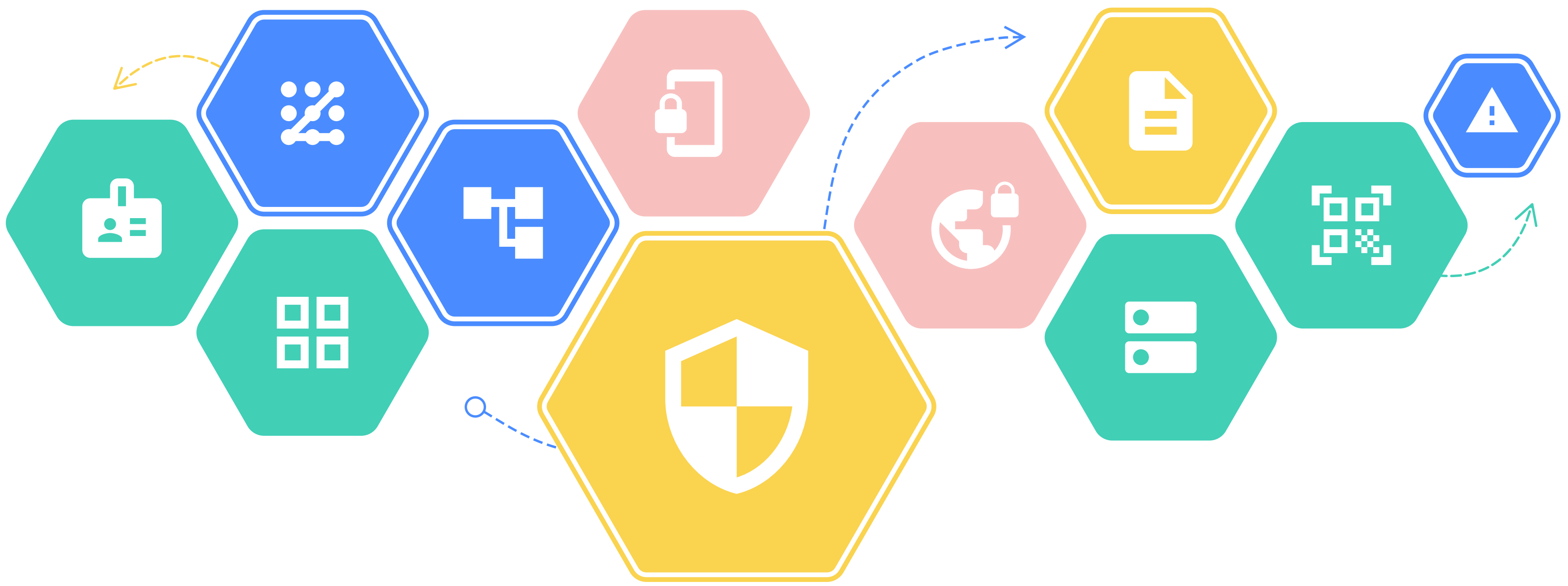
Compliance automation software can also bring costs down significantly by making the entire process more efficient.

Secureframe streamlines the process of building a compliant ISMS. Our library of auditor-approved policy templates, automated evidence collection, and simplified risk management frees your team up to focus on high-priority projects. And our in-house compliance experts can save you thousands of dollars on consultant fees and readiness assessments.

ISO 27001 controls and requirements

Security controls are the processes and policies you put in place to minimize risk. ISO 27001 Annex A includes 114 controls, divided into 14 categories.

ISO 27001 Control Categories



- Information security policies
- Organization of information security
- Human resources security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, & maintenance
- Supplier relationships
- Incident management
- Business continuity management
- Compliance

How you satisfy Annex A control requirements will depend on your unique business. The ISO 27001 standard allows organizations to meet the requirements in their own way.

If you choose not to include an Annex A control, explain why in your Statement of Applicability. For example, if you chose to exclude A.6.2.2 because none of your employees work remotely, your certification auditor will want to know.

Besides meeting Annex A control requirements, organizations must satisfy clauses 4-10 of the ISO 27001 standard document.

Clause 4: Context of the organization

Why does your company handle information assets in the first place, and what do you use them for?

Your auditor can't assess the effectiveness of your ISMS if they don't understand its goals. Document what your organization does, what customers need from you, and the scope of your ISMS.

Clause 5: Leadership

Auditors want to know that company leaders are accountable for the success of the ISMS. Senior managers will need to commit to monitoring, testing, and improving information security processes.

Clause 6: Planning

Clause 6 deals with risk management. Documentation should show:

- How you identify and analyze information security risk
- Your process for choosing how to respond to each risk
- What risk avoidance, tolerance, and mitigation look like for your organization

Clause 7: Support

ISO 27001 requires a sophisticated ISMS, and that demands a lot of support. Clause 7 asks for a plan to ensure resources will always be available to sustain the system properly.

Clause 8: Operations

Clause 8 builds on the requirements of Clause 6 to discuss how risk assessments are implemented. You'll need to create a document that pulls together the elements laid out in Clauses 6 and 7 into a coherent, start-to-finish plan.

Clause 9: Performance evaluations

Document how you'll measure the effectiveness of your ISMS, such as regular penetration tests. You'll also need a plan for conducting internal audits to ensure you remain ISO 27001 compliant after your certification audit is complete.

Clause 10: Improvement

Clause 10 is all about damage control. How do you react if you spot a nonconformity in your ISMS? Once you've resolved an issue, how do you shore up the system so it doesn't happen again? A good ISMS is in a constant state of growth and improvement.

Part III: Automating ISO 27001 Certification with Secureframe

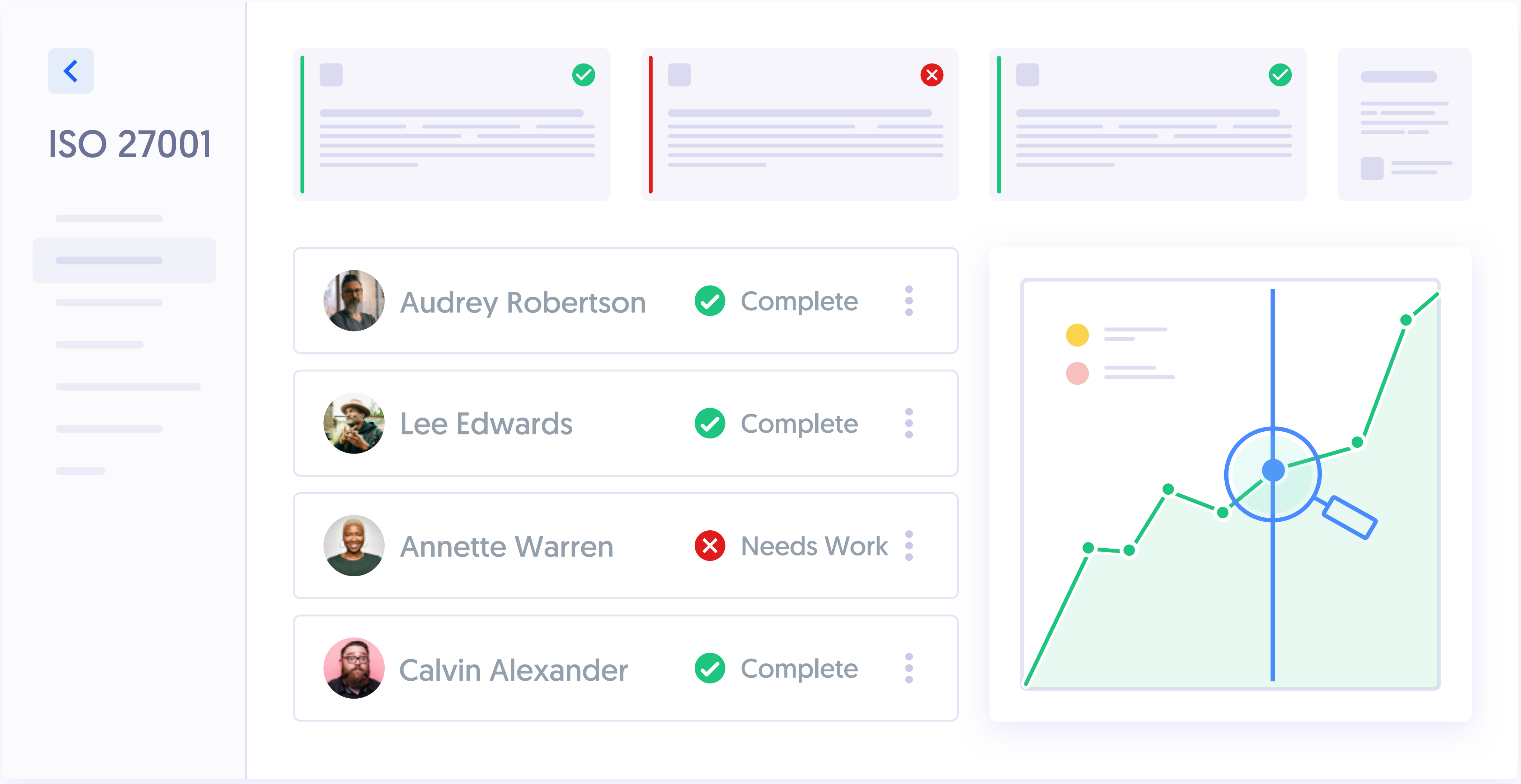
The traditional route to ISO 27001 certification is time-consuming, tedious, and stressful.

Normally, you'd need to complete a thorough risk assessment and gap analysis, then design controls and write policies from scratch. You'd need to train your staff on security best practices and make sure they all review the new policies. And you'd have to update spreadsheets and grab hundreds of screenshots to use as evidence during your formal audit.

It all means dedicating multiple team members and company leaders to overseeing compliance, and likely hiring a consultant to assist you.

Compliance automation software can do a lot of this heavy lifting for you, saving hundreds of hours and thousands of dollars on audit preparation and consultant fees.

- Secureframe integrates with your existing tech stack to automatically collect evidence. Onboarding workflows guide your team through security training and policy review so you don't have to remind them.
- Compliance dashboards give you a real-time view of how close you are to being audit-ready.
- In-house ISO 27001 experts are with you every step of the way, helping you implement controls and offering tailored advice based on your company's unique requirements.



Audrey Robertson ✓ Complete

Lee Edwards ✓ Complete

Annette Warren ✗ Needs Work

Calvin Alexander ✓ Complete

	With Secureframe	Without Secureframe
Your Team's Time Commitment	~40 hours and streamlined audits Your Stage 1 and Stage 2 audits will be quick and seamless, since you'll be working with Auditor Partners familiar with our automated evidence collection process.	150-200+ hours and longer audits ISO 27001 is a major undertaking with a lot of moving parts. It normally requires executive buy-in and frequent meetings to ensure preparation stays on schedule.
Audit Project Management and Evidence Collection	Secureframe integrates with core services like Gusto, GSuite, Github, AWS, Google Cloud, and Azure to automatically assess security practices and implement controls. We continuously collect audit evidence, run security awareness training, and more.	Assign individual evidence collection tasks to team members and consultant, typically across project management, spreadsheet, and ticketing systems. Manual evidence collection includes screenshots and cron jobs.
Controls and Policies	Use our library of auditor-approved policies and templates to meet ISO 27001 requirements and get audit ready faster.	Work with a consultant to build policies and collect documentation for dozens of controls.
Vendor Management	Track and monitor vendor environments, risks, and compliance reports.	Manual, time consuming vendor management process. May take weeks or months to get a security questionnaire response.
Customer Compliance Package	We collect your audit readiness materials into a Customer Compliance Package right after onboarding so you can accelerate your sales cycle while completing your ISO 27001 certification.	May need to talk to lawyers and/or pay your consultant extra to create a Customer Compliance Package.

Part IV: ISO 27001 Readiness Checklist

Step 1 Appoint an ISO 27001 team

- □ Establish roles, responsibilities, and timelines for certification
- □ Define the scope of your ISMS and consult with company leadership

Step 2 Create and publish ISMS policies, documents, and records

- □ Build a framework for establishing, implementing, maintaining, and improving the ISMS
- □ Consult with senior management to establish an information security policy that explains how you'll protect the confidentiality, integrity, and availability of your information assets
- □ Include references to supporting documentation:
  - □ Information Security Objectives
  - □ Leadership and Commitment
  - □ Roles, Responsibilities, and Authorities
  - □ Approach to Assessing and Treating Risk
  - □ Control of Documented Information
  - □ Communication
  - □ Internal Audit
  - □ Management Review
  - □ Corrective Action and Continual Improvement
  - □ Policy Violations
- □ Finalize and publish policies for employees to review

Step 3 Conduct a risk assessment

- □ Establish a risk management framework
- □ Identify potential information security risks
- □ Determine the likelihood each risk could occur
- □ Evaluate the potential impact of identified risks
- □ Rank risks based on likelihood and impact
- □ Create a response plan for each risk
- □ Assign an owner to each risk

Step 4 Complete a Statement of Applicability

- □ Review the 114 controls of Annex A
- □ Select controls to address identified risks using ISO 27002 as a reference
- □ Complete the Statement of Applicability listing all Annex A controls, justifying inclusion or exclusion of each control

Step 5 Implement ISMS policies and controls

- □ Create a communication plan to inform staff of changes and progress
- □ Share policies and track employee review
- □ Monitor control effectiveness

Step 6 Train team members on ISO 27001

- □ Conduct regular trainings to ensure awareness of new policies and procedures
- □ Define expectations for personnel regarding their role in maintaining the ISMS
- □ Train personnel on common threats facing your organization and how to respond
- □ Establish disciplinary policies/processes for personnel who violate information security requirements

Step 7 Gather documentation and evidence

- □ Prepare an ISO 27001 Required Documents and Records list to reference during your audit

Step 8 Undergo an Internal Audit

- □ Identify scope and methodology of internal audit (Clauses 4-10 and applicable Annex A controls)
- □ Choose an independent, objective internal auditor
- □ Produce and record internal audit results
- □ Remediate any internal audit findings

Step 9 Undergo a Stage 1 audit

- □ Select an accredited ISO 27001 auditor
- □ Conduct a Stage 1 Audit. Auditor will complete an extensive documentation review to evaluate ISMS design
- □ Gauge readiness for a Stage 2 Audit

Step 10 Implement Stage 1 audit advice

- □ Ensure that all ISO 27001 requirements are addressed
- □ Ensure org is following documented processes
- □ Ensure org is upholding contractual requirements with third parties
- □ Record and address nonconformities identified by the auditor

Step 11 Undergo a Stage 2 audit

- □ Conduct Stage 2 audit. Auditor will test ISMS to ensure proper design and functionality as well as evaluate implementation and operation of clauses 4-10 and applicable Annex A controls

Step 12 Implement Stage 2 audit advice

- □ Ensure that all ISO 27001 requirements are addressed
- □ Ensure org is following documented processes
- □ Ensure org is upholding contractual requirements with third parties
- □ Record and address nonconformities identified by the auditor

Step 13 Commit to subsequent audits and assessments

- □ Hold quarterly or bi-annual management reviews
- □ Prepare for first and second year surveillance audits
- □ Perform annual risk assessments and internal audit
- □ Prepare for year three recertification audit
- □ Ensure the ISMS and its objectives remain effective

Step 14 Perform ongoing improvements

- □ Ensure weaknesses/threats to the ISMS are identified and addressed
- □ Document and track nonconformities and remediation

The smart way to get ISO 27001 compliant

Secureframe is the all-in-one platform for integrated security compliance and audit readiness.

Trusted by today's leading companies

stream Lob dooly. Doodle CloudApp

INSTABASE fabric trusted TopFunnel slab

Build your ISMS

We help you design an ISMS that aligns with ISO 27001 standards and your organization's needs. Select from our library of 40+ policies, adapt them for your organization, and publish for your employees to review.

Secure your cloud infrastructure

We connect with and monitor 150+ cloud services, including AWS, Google Cloud, and Azure, to help ensure compliance. You'll be notified of any vulnerabilities and get specific instructions for fixing them.

Get audit-ready fast

We streamline audit prep with automated evidence collection from 100+ integrations, plus seamless evidence submission workflows with auditors. Evidence is automatically collected for you throughout the year, making surveillance and recertification audits simpler and easier.

Ready to get your ISO 27001 certification?

Request a demo of Secureframe today