Vanta

The ISO 27001 Compliance Checklist

The ISO 27001 Compliance Checklist

ISO 27001 is the global gold standard for ensuring the security of information and its supporting assets. Obtaining ISO 27001 certification can help an organization prove its security practices to potential customers anywhere in the world.

Our ISO 27001 checklist will help your organization successfully implement an Information Security Management System (ISMS) according to the standard, and prepare your org for an independent audit of your ISMS to obtain ISO 27001 certification. Let's get started!

STEP 1

Develop a roadmap for your ISMS implementation and ISO 27001 certification

Creating a plan for your implementation is the first step toward getting ISO 27001 certified. After you've purchased the ISO 27001 standard and ISO 27002, the guide for implementing ISO 27001, you will need to start organizing your implementation project, including these tasks:

- □ Implement a plan, do, check, act (PDCA) process to identify challenges and gaps for remediation.
- □ Consider the costs of ISO 27001 certification relative to your organization's size and number of employees.
- □ Use project planning tools like project management software, Gantt charts, or Kanban boards.
- □ Define the scope of work from planning to completion.

STEP 2

Determine the s cope of your organization's ISMS

Each organization's ISO 27001 certification process will vary depending on how you set up your ISMS. The scope of your ISMS will depend on how big your organization is, the type of data you're handling, the ways you process or interact with that data, and so on. These steps can help you establish the scope of your ISMS:

- □ Decide which business areas are covered by your ISMS and which ones are out of scope.
- □ Consider additional security controls for processes that are required to pass ISMS-protected information across the trust boundary.
- □ Communicate the scope of your ISMS to stakeholders.

STEP 3

Establish an ISMS team and assign roles

Now that you have a clear understanding of what your ISMS will cover, establish a team that will build this ISMS. This may include internal employees like engineers and compliance specialists, external contractors, or a combination of both depending on your needs.
For this phase, follow these steps:

□ Select engineers and technical staff with experience in information security to construct and implement the security controls needed for ISO 27001.

□ Build a governance team with management oversight.

□ Incorporate key members of top management (senior leadership and executive management) and assign responsibility for strategy and resource allocation.

If you have a large team, consider assigning a dedicated project manager to track progress and expedite implementation. Align the team on the following:

□ The planning steps you've already taken.

□ The scope of the ISMS.

□ Which team members are responsible for which aspects of the project.

STEP 4

Conduct an inventory of information assets

Before your team starts working, you need to ensure everyone has a clear understanding of what assets the ISMS will be protecting.
Use this checklist to take inventory of the data you need to secure:

□ Consider all assets where information is stored, processed, and accessible, including: record information assets like data and people, record physical assets like laptops, servers, and physical building locations, and record intangible assets like intellectual property, brand, and reputation.

□ Assign each asset a classification and an owner to ensure they are all appropriately inventoried, classified, protected, and handled.

□ Meet with your team to discuss this inventory and ensure that everyone is aligned.

STEP 5

Perform a risk assessment

The next step is to perform a thorough risk assessment. Follow these steps to identify and analyze the risks facing your organization:

□ Establish and document a risk management framework to ensure consistency.

□ Identify scenarios in which information, systems, or services could be compromised.

□ Determine the likelihood or frequency with which these scenarios could occur.

□ Evaluate the potential impact of each scenario on the confidentiality, integrity, or availability of your data, systems, and services.

□ Rank risk scenarios based on overall risk to the organization's objectives.

STEP 6

Develop a risk register

After conducting a detailed risk assessment, turn the findings into a practical record. With your ISO 27001 certification team, check off these items to create a viable risk register:

□ Record and manage your organization's risks that you identified during your risk assessment.

□ Summarize each identified risk.

□ Indicate the impact and likelihood of each risk.

□ Rank risk scenarios based on overall risk to the organization's objectives.

STEP 7

Document a risk treatment plan

The next step is to address and mitigate the risks you've identified. Follow these steps to start taking action:

□ Design a response for each risk, known as a risk treatment.

□ Assign an owner to each identified risk and each risk mitigation activity.

□ Establish target timelines for completion of risk treatment activities.

□ Implement your risk mitigation treatment plan and track the progress of each task.

STEP 8

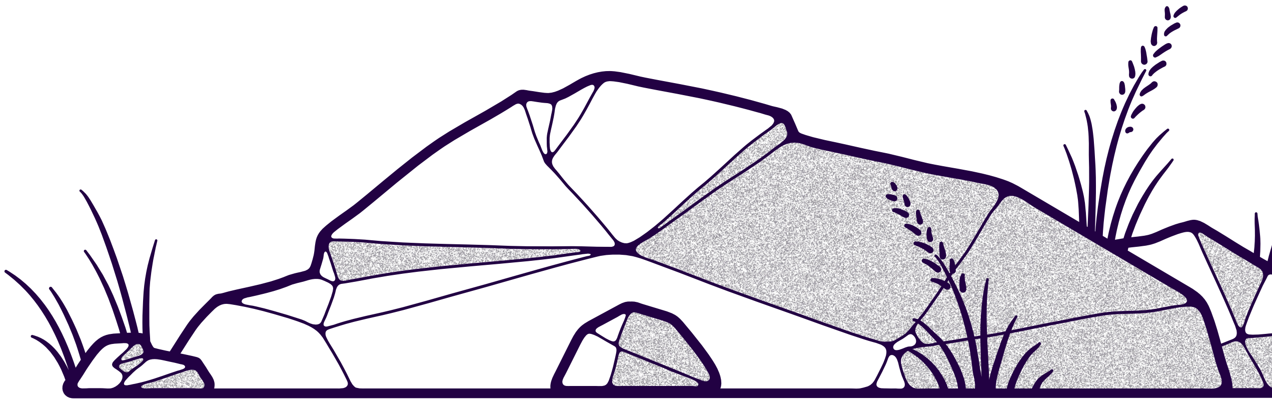
Complete the Statement of Applicability

Annex A is a section of the ISO 27001 standard that lists the security controls and practices that you should consider implementing to meet the compliance requirements. These controls are selected based on risk or your organization's requirements — some may be excluded from your ISMS if they aren't relevant to your environment. As part of your compliance process, you'll need to complete a report called the Statement of Applicability that explains which of the Annex A controls that are in scope for your ISMS. Follow these steps to create this document:

□ Review the 93 controls listed in Annex A.

□ Select the controls that are relevant to the risks you identified in your risk assessment.

□ Complete the Statement of Applicability listing all Annex A controls, justifying inclusion or exclusion of each control in your ISMS implementation.



STEP 9

Implement ISMS policies, controls and continuously assess risk

After completing the Statement of Applicability and your initial risk assessment, you should have a clear understanding of how to move forward with your ISO 27001 compliance. Follow these steps and address each of the controls included in your Statement of Applicability:

□ Assign owners to each of the security controls to be implemented.

□ Figure out a way to track the progress and goals for each control.

□ Build a framework for establishing, implementing, maintaining, and continually improving the ISMS.

Include information or references to supporting documentation regarding:

□ 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

□ Corrective action and continual improvement

□ Policy violations

□ All of the Annex A controls that you have selected

STEP 10

Establish employee training

Any employee at your organization could unknowingly give hackers access to your data, so a core part of ISO 27001 compliance is training employees to prevent fraud and data theft. Follow these steps to train your employees on data security and establish a plan to continue these trainings.

□ Define expectations for personnel regarding their role in ISMS maintenance.

□ Train personnel on common threats facing your organization and how to respond.

□ Establish disciplinary or sanctions policies or processes for personnel found out of compliance with information security requirements.

□ Make security training part of the onboarding process for new employees.

□ Conduct regular training to ensure awareness of new policies and procedures.

STEP 11

Conduct regular management reviews

To maintain your ISO 27001 compliance, you need to monitor and update your system on a regular basis. You may break your compliance unintentionally when you make updates to your network, when a certain tool stops working, when you stop following particular policies, or through other errors and changes. Follow these steps to maintain your ISO 27001 compliance:

- □ **Plan reviews at least once per year. Consider a quarterly review cycle if your organization is large or if your infrastructure is changing frequently.**
- □ **Ensure the ISMS and its objectives continue to be effective.**
- □ **Verify that senior management stays informed.**
- □ **Ensure risks or deficiencies can be promptly addressed.**

STEP 12

Assemble ISO 27001 required documents

After you've implemented the necessary security controls and practices from Annex A, begin preparing for your ISO 27001 audit. Start collecting the documentation for your audit by following these steps:

- □ **Review the ISO 27001 Required Documents and Records list.**
- □ **Customize policy templates with organization-specific policies, process, and language.**

STEP 13

Perform an ISO 27001 internal audit

To ensure you'll pass your official audit, conduct an internal audit to make sure you've addressed all areas of non-compliance. Complete these tasks for your internal review:

- □ **Examine each of the requirements from Annex A that you deemed applicable in your ISMS' Statement of Applicability and verify that you have each in place.**
- □ **Assign in-house employees to conduct the internal audit, specifically employees who were not involved in the ISMS development and maintenance or hire an independent third party.**
- □ **Share internal audit results, including nonconformities, with the ISMS team and senior management.**
- □ **Address any issues your internal audit identified before proceeding with the external audit.**
- □ **Verify compliance with the requirements from Annex A deemed applicable in your ISMS' Statement of Applicability.**

STEP 14

Undergo external audit of ISMS to obtain ISO 27001 certification

Now you're ready to pursue your official ISO 27001 certification. Follow these steps for your external audit:

- □ **Select an independent ISO 27001 auditor.**
- □ **Complete the Stage 1 Audit consisting of an extensive documentation review; obtain the auditor's feedback regarding your readiness to move to the Stage 2 Audit.**
- □ **Complete the Stage 2 Audit consisting of tests performed on the ISMS to ensure proper design, implementation, and ongoing functionality; evaluate fairness, suitability, and effective implementation and operation of controls.**

STEP 15

Address any nonconformities

If issues arise during your ISO 27001 audit, your auditor will explain these nonconformities. Follow these steps:

- □ **Ensure that all requirements of the ISO 27001 standard are addressed.**
- □ **Ensure your organization is following the processes that it has specified and documented.**
- □ **Ensure your organization is upholding contractual requirements with third parties.**
- □ **Address specific nonconformities identified by the ISO 27001 auditor.**
- □ **Receive auditor's formal validation following resolution of nonconformities.**

If your auditor does not find any nonconformities, you can skip this step.

STEP 16

Plan for subsequent ISO 27001 audits and surveillance audits

To maintain your ISO 27001 certification, you'll need to pass surveillance audits every year and undergo a full audit every three years. Keep these timelines in mind:

- □ **Prepare to perform surveillance audits every year of your certification cycle.**
- □ **Perform a full ISO 27001 audit once every three years.**

STEP 17

Consider streamlining ISO 27001 certification with automation

To ensure you're always ISO 27001 compliant, use a compliance automation platform that helps your organization stay secure. A compliance automation platform provides ongoing monitoring to notify you anytime your organization falls out of compliance.

Vanta's trust management platform provides guidance with step-by-step instructions for identifying gaps and implementing the ISO 27001 controls. Vanta automates up to 80% of the work required to obtain ISO 27001.

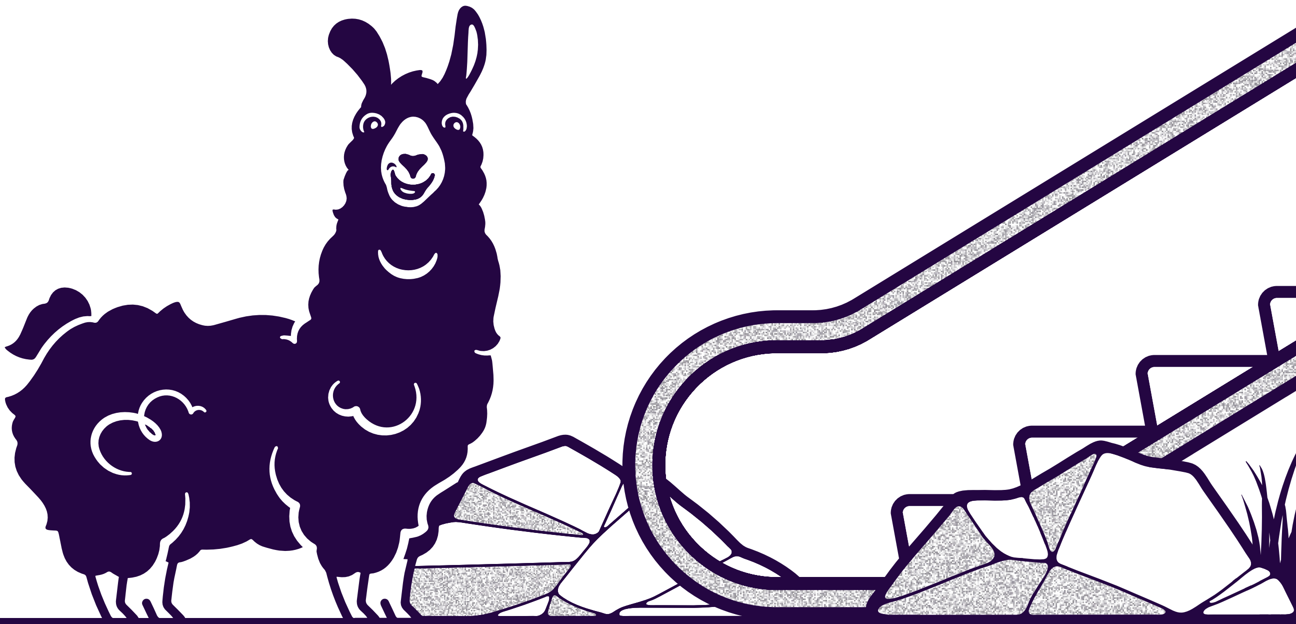
See how you can automate your ISO 27001 implementation by requesting a demo.

Prioritizing your security and opening doors with ISO 27001 compliance

Information security is a vital priority for any business today from an ethical standpoint and from a business standpoint. Not only could a data breach jeopardize your revenue, but many of your future clients and partners may require an ISO 27001 report before they consider your organization. Achieving and maintaining your ISO 27001 compliance can open countless doors, and you can simplify the process with the help of the checklist above and Vanta's compliance automation software.

Request a demo today to learn more about how we can help you protect and grow your organization.

Request a demo →



Vanta

Automate compliance. Simplify security. Demonstrate trust.

Vanta is the leading trust management platform that helps simplify and centralize security for organizations of all sizes. Thousands of companies rely on Vanta to build, maintain and demonstrate their trust—all in a way that's real-time and transparent. Founded in 2018, Vanta has customers in 58 countries with offices in Dublin, New York, San Francisco and Sydney.

For more information, visit: www.vanta.com | sales@vanta.com