Your ISO 27001 Audit Readiness Checklist

The Vanta team has supported companies through thousands of audits to achieve SOC 2, ISO 27001, HIPAA, PCI, and GDPR compliance. We will apply our expertise and know-how to guide you through a successful audit quickly.

Company Settings | Audits

The Audits page is where you include information about your company, add users, and set up API integrations. Additionally, you can confirm your audit has been entered into Vanta correctly.

- □ Grant access to your auditor (This lets the auditor know that you want to engage with them. Don't worry, they won't get access to your instance until your audit window starts!)
- □ Verify your auditor has successfully added your audit to the Vanta platform.
- □ Confirm the details of your audit: type, start date, and auditor.
- □ If there is missing information, please contact your Customer Success Manager or auditor to rectify .

Personnel | People

The People page in the Personnel section is where auditors would see your employees and their task status. They will want to see that employees are completing their onboarding tasks and employees who left are offboarded correctly.

- □ Please refer to the checklists section to set up onboarding/offboarding tasks for Employees.
- □ It would be great to set these up correctly and make sure employees have completed all tasks before the audits.
- □ If there are any service accounts/employees with no tasks, please be ready to explanations for this ie. They are non working employees etc.

Personnel | Computers

The Computers page in the Personnel section is where auditors would see your endpoint devices used by employees. They will want to see that these computers are set up correctly from a security point of view.

- □ These are tracked via your MDM solution whether that is an integration or via the Vanta Agent if you are using this.
- □ If you are using an MDM which is not yet integrated with Vanta please attach a custom document showing similar testing (ie. Employee laptops are hardware encrypted, anti virus installed etc.) as auditors would want to see this.

Policies

Policies are the foundation of your security program. This section ensures the review and approval of all policies within the last year, which is crucial for any audit you perform.

- □ Review your policies using the eye icon on the right side of the screen.
- □ The approved date for all policy PDFs should be within the last 12 months.
- □ Confirm you have read all policies before your audit begins.
- □ Configure SLAs and ensure that they are aligned with approved policies.

Vulnerabilities

Vulnerability scanning is a crucial control for any audit. This section guides you through the data needed to provide sufficient evidence to your auditor.

- □ If you use a 3rd party scanning tool for vulnerabilities and do not integrate with Vanta, you will need to upload screenshots for the auditor. If you have any open high or medium vulnerabilities, you need to show a clear plan to remediate during the audit.
- □ In-scope vulnerabilities must be resolved or have a remediation plan that is in accordance with your Operations Security Policy (or equivalent). You may deactivate monitoring for out of scope vulnerabilities. Reach out to your auditor to confirm scoping before deactivating monitoring.
- □ Review the SLA misses tab to confirm their acknowledgment.
- □ If you are not using an integrated service for vulnerability scanning, check the documents tab for how to upload:
  - □ Vulnerabilities Remediated Sample
  - □ Vulnerability Scan

Documents Tab

You will also need to provide documents, manual evidence that can't be automated. Be sure all documents are accurate, up-to-date and uploaded.

- □ Upload the documents specified by your auditor to Vanta. Different auditors have different requirements. The document requirements will be customized depending on the auditor that you choose. Therefore, it's important to add your auditor sooner than later!

Access

Access control is a fundamental component of data security that limits who can access and use company information and resources.

- □ Link all user accounts with employees in Vanta to pass this control.
- □ Verify all user accounts link to individual employees and not a shared account.
- □ Track this for all possible integrations from the drop-down menu:
  - □ Cloud Infrastructure
  - □ Identity Providers
  - □ Version Control

If you have Access Reviews enabled, complete the following:

- □ Set up a schedule to automate the creation of access reviews.
- □ Create access reviews manually, if needed.
- □ Ensure that each review has a designated owner assigned.

Risk Management

Review all of the risks that have been identified for your business. For each risk, review and describe the risk treatment plan.

- □ Configure your risk management Settings.
- □ Upload existing risks or select risks from the risk Library.
- □ Review the risk Register, assign owner and complete assessment for each risk.
- □ Create a snapshot for audit evidence.

Vendors

Assessing the security controls for vendors who have access to your sensitive data is vital to any audit.

- □ Ensure all in-scope vendors are listed. Manually add vendors if needed.
- □ Add SOC 2 report, SOC 3 report, or ISO 27001 certification for in-scope vendors. Confirm all security questionnaires are complete unless a SOC 2 report, SOC 3 report, or ISO 27001 certification is uploaded.
  - □ Note: Best practice is to review the SOC 2 report or ISO 27001 certification, SOC 3's should only be used for vendor reviews when a SOC 2 isn't available.
- □ Complete Comments on vendor security controls to demonstrate that you have read and understood the security documentation and have determined the security of the external vendor meets the required security controls standards.
  - □ Example: "AWS SOC 2 report meets expectations and requirements. All services in scope." or "Exception in AWS SOC 2 report noted, does not affect the use of service."
- □ Add the vendor review date.

Frameworks & Controls

The Frameworks page serves as a dashboard to showcase progress for both Vanta's standard frameworks and any custom frameworks you've created. The Controls page provides a centralized list of controls across all enabled frameworks.

- □ Add any custom controls if needed.
- □ Ensure that all controls have assigned owners.
- □ Carefully review the control language with control owners to help them understand their roles and responsibilities, e.g., HR Teams, Engineers, etc.
  - □ **Example:** An auditor may ask your team member to explain the onboarding process. The auditor will compare the onboarding process to determine whether it is effective and whether it is operating properly, that is, whether you can demonstrate that you have an effective onboarding policy and whether you follow that policy with the procedures you perform when you hire someone.

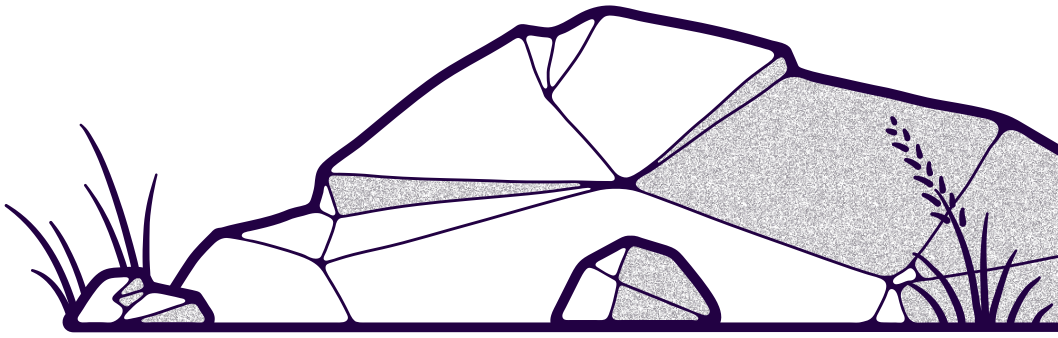
Internal Audit overview

The internal audit is an important aspect of your ISO 27001 certification. An ISO 27001 internal audit involves examining an organization's Information Security Management System (ISMS) before undergoing an ISO audit with an external auditor. The internal audit aims to help identify gaps or deficiencies that could affect an organization's ISMS and impact its ability to meet its intended objectives and complete an initial or annual ISO 27001 certification audit.

Before the Internal Audit:

Ensure the following items are completed before you conduct your internal audit:

- □ In-scope systems integrated and scopes configured appropriately.
- □ Create custom controls, tests and documents, if needed.
- □ Assign owners to all controls, tests and documents.
- □ Remediate relevant automated tests (mark as irrelevant if not in–scope).
- □ Complete and upload as many documents as you can to showcase your compliance.
- □ Policies drafted, approved and accepted by required employees.
- □ Configured SLAs match with approved policies.
- □ Define risk management settings and complete the risk assessment.
- □ Access: All accounts are assigned to a user.
- □ Vulnerabilities: Resolve or plan for resolution of in-scope vulnerabilities.
- □ Complete the vendor listing, vendor information.
- □ Conduct and ensure you have completed a management review of your ISMS.



Before the External Audit:

As a reminder the External Audit is a two part exercise:

- → **Stage 1** - In this first stage of your audit, your auditor will review the documentation you've provided that maps out your ISMS and details the security controls you have in place. At this stage, the auditor will provide you with corrective action to take or will move into the next stage of the audit.
- → **Stage 2** - In this second stage of the audit is when your auditor will thoroughly investigate your ISMS to verify you're following each of the ISO 27001 requirements. If you pass this stage, you will officially receive your ISO 27001 certification. While the auditor will lead the auditing process, you will still need to be involved to answer questions about your ISMS, provide additional documentation, and respond to any other requests that they have.

Ensure the following items are also completed before you conduct your external (Stage 1 and 2) audits:

☐ In-scope systems integrated and scopes configured appropriately.

☐ Review internal audit report and make any recommended changes

☐ Be sure to add internal audit non-conformities to the nonconformities tracker

☐ Upload the internal audit report to the Internal Audit Report

Once the External Audit Begins

As soon as your external audit begins, you need to understand what you can and cannot do within Vanta to comply with your audit.

☐ **DO NOT** disable any tests on the Tests page—if this is needed, please contact your auditor.

☐ **DO NOT** scope any users or systems out on the Connections page.

☐ **DO NOT** enable any Development or Test environment resources on the Connections page.

☐ **DO NOT** disable any Production environment resources on the Connections page.

☐ **DO NOT** change the SLAs on the SLA's page.

☐ **DO NOT** alter any uploaded documents including, but not limited to, policies, organization charts, job descriptions, etc.

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**