The 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 .

Policies

Policies are the foundation of your security program. This section ensures the creation 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 created date for all policy PDFs should be within the previous 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.

Vulnerabilities (cont.)

- [ ] Review the SLA violations 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

If you are not self-attesting, your auditor may request documents in line with your organization's policies (auditors ask "Is there policy?", "Is it effective?", "Is it operating properly?"), 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 Assessment

Effectively completing the risk assessment is imperative to any audit using Vanta. It offers organizations several benefits, such as protecting assets and optimizing data security.

- [ ] 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.

- [ ] Add SOC 2 report, SOC 3 report, or ISO 27001 certification for all your 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.
- [ ] Ensure all in-scope vendors are listed. Manually add vendors if needed.

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.

Before the Observation Window Begins

Before your Observation Window begins, you need to ensure that only production environment systems are marked as in-scope on the integrations page.

- [ ] Confirm Vanta links to all in-scope systems.
  - [ ] Confirm that all resources in the production environment of integrated systems are marked as in-scope.
  - [ ] Confirm that all resources in the Development and Test environment of integrated systems are marked as out of scope.
- [ ] 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 all pre-audit documents.
  - [ ] **Tip:** Use the 'Time sensitivity' filter to identify document requests that should wait until the audit period starts.
- [ ] Policies drafted, approved and accepted by required employees.

Before the Observation Window Begins (cont.)

- [ ] 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.

Once the Observation Window Begins

As soon as your Observation Window starts, 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 Integrations page.
- [ ] **DO NOT** enable any Development or Test environment resources on the Integrations page.
- [ ] **DO NOT** disable any Production environment resources on the Integrations 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.