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 successful implementation of an ISMS and ISO 27001 certification

- [ ] Implement Plan, Do, Check, Act (PDCA) process to recognize challenges and identify gaps for remediation
- [ ] Consider ISO 27001 certification costs relative to org size and number of employees
- [ ] Clearly define scope of work to plan certification time to completion
- [ ] Select an ISO 27001 auditor

STEP 2

## Set the scope of your organization's ISMS

- [ ] Decide which business areas are covered by the ISMS and which are out of scope
- [ ] Consider additional security controls for business processes that are required to pass ISMS-protected information across the trust boundary
- [ ] Inform stakeholders regarding scope of the ISMS

STEP 3

## Establish an ISMS governing body

- [ ] Build a governance team with management oversight
- [ ] Incorporate key members of top management, e.g. senior leadership and executive management with responsibility for strategy and resource allocation

STEP 4

## Conduct an inventory of information assets

- [ ] Consider all assets where information is stored, processed, and accessible
    - → Record information assets: data and people
    - → Record physical assets: laptops, servers, and physical building locations
    - → Record intangible assets: intellectual property, brand, and reputation
- [ ] Assign to each asset a classification and owner responsible for ensuring the asset is appropriately inventoried, classified, protected, and handled

STEP 5

## Execute a risk assessment

- [ ] Establish and document a risk-management framework to ensure consistency
- [ ] Identify scenarios in which information, systems, or services could be compromised
- [ ] Determine likelihood or frequency with which these scenarios could occur
- [ ] Evaluate potential impact of each scenario on confidentiality, integrity, or availability of information, systems, and services
- [ ] Rank risk scenarios based on overall risk to the organization's objectives

STEP 6

## Develop a risk register

- [ ] Record and manage your organization's risks
- [ ] Summarize each identified risk
- [ ] Indicate the impact and likelihood of each risk

STEP 7

## Document a risk treatment plan

- [ ] Design a response for each risk (Risk Treatment)
- [ ] Assign an accountable owner to each identified risk
- [ ] Assign risk mitigation activity owners
- [ ] Establish target dates for completion of risk treatment activities

STEP 8

## Complete the Statement of Applicability worksheet

- [ ] Review 114 controls of Annex A of ISO 27001 standard
- [ ] Select controls to address identified risks
- [ ] Complete the Statement of Applicability listing all Annex A controls, justifying inclusion or exclusion of each control in the ISMS implementation

---

STEP 9

## Create an Information Security Policy, the highest-level internal document in your ISMS

- [ ] 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
  - → Policy Violations

---

STEP 10

## Assemble required documents and records

- [ ] Review ISO 27001 Required Documents and Records list
- [ ] Customize policy templates with organization-specific policies, process, and language

STEP 11

## Establish employee training and awareness programs

- [ ] Conduct regular trainings to ensure awareness of new policies and procedures
- [ ] 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

STEP 12

## Perform an internal audit

- [ ] Allocate internal resources with necessary competencies who are independent of ISMS development and maintenance, or engage an independent third party
- [ ] Verify conformance with requirements from Annex A deemed applicable in your ISMS's Statement of Applicability
- [ ] Share internal audit results, including nonconformities, with the ISMS governing body and senior management
- [ ] Address identified issues before proceeding with the external audit

STEP 13

## Undergo external audit of ISMS to obtain ISO 27001 certification

- [ ] Engage an independent ISO 27001 auditor
- [ ] Conduct Stage 1 Audit consisting of an extensive documentation review; obtain feedback regarding readiness to move to Stage 2 Audit
- [ ] Conduct 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 14

## Address any nonconformities

- [ ] Ensure that all requirements of the ISO 27001 standard are being addressed
- [ ] Ensure org is following processes that it has specified and documented
- [ ] Ensure org 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

STEP 15

## Conduct regular management reviews

- [ ] Plan reviews at least once per year; consider a quarterly review cycle
- [ ] Ensure the ISMS and its objectives continue to remain appropriate and effective
- [ ] Ensure that senior management remains informed
- [ ] Ensure adjustments to address risks or deficiencies can be promptly implemented

STEP 16

## Calendar ISO 27001 audit schedule and surveillance audit schedules

- [ ] Perform a full ISO 27001 audit once every three years
- [ ] Prepare to perform surveillance audits in the second and third years of the Certification Cycle

STEP 17

## Consider streamlining ISO 27001 certification with automation

- [ ] Explore tools for automating security and compliance
- [ ] Transform manual data collection and observation processes into automated and continuous system monitoring
- [ ] Identify and close any gaps in ISMS implementation in a timely manner

STEP 18

## Learn more about achieving ISO 27001 certification with Vanta

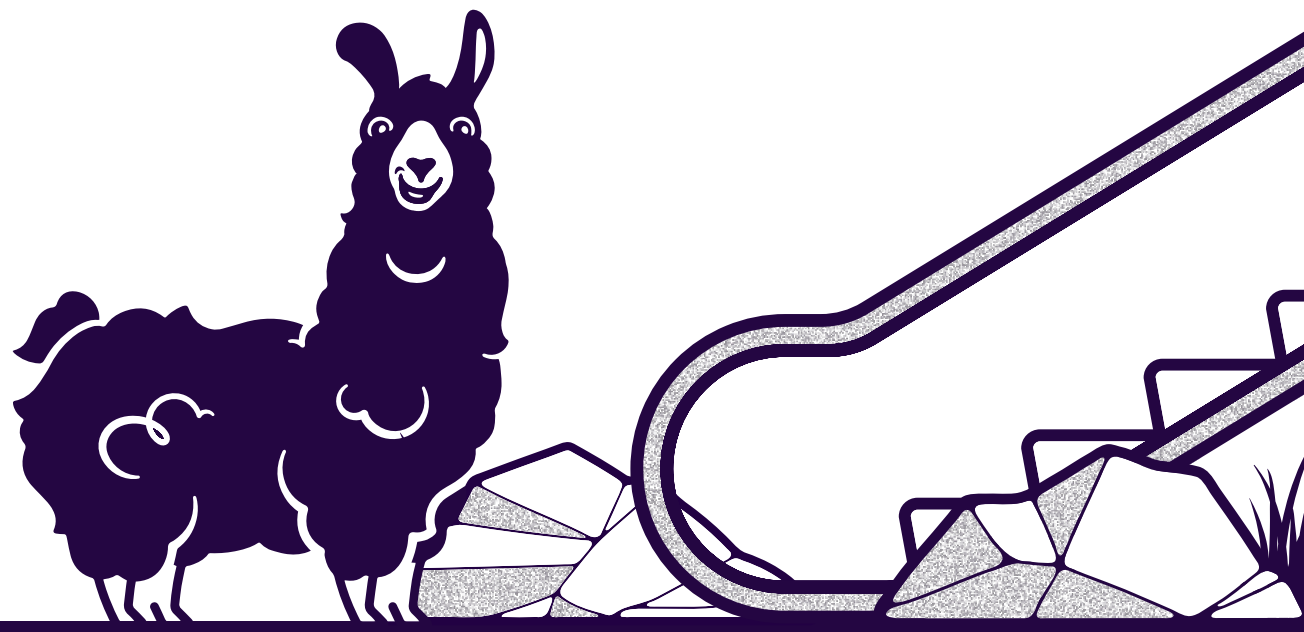
- [ ] Book an ISO 27001 demo with Vanta

## 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**