DRATA

ISO 27001 Checklist

The number of companies that achieve ISO 27001 certification each year is growing as businesses expand to different global markets. However, ISO 27001 comes with its own set of challenges for teams trying to achieve certification for the first time.

To help get you started, we put together this high-level ISO 27001 checklist covering the main milestones on the way to compliance.

STEP 1

Develop an Implementation Team and Project Plan

Create a team of people to implement your ISMS, including members from various areas of the organization.

This team may include:

> A project manager
>
> Representatives involved in the development and implementation of the ISMS (ex: information security)
>
> Representatives from technical groups (ex: network engineers)
>
> Appropriate members of the leadership team

Action items:

- [ ] Establish roles and responsibilities for team members

STEP 2

Understand ISO 27001 Requirements

Action items:

- [ ] Review each clause of ISO 27001
- [ ] Review Annex A of ISO 27001

STEP 3

Find Your Security Baseline

Action items:

- [ ] Understand the current state of security in your organization by asking the following questions:
  - [ ] What is currently working, and what processes do you already have in place that will support your certification?
  - [ ] What's not working? Are there any gaps you're aware of that create security risks?
  - [ ] Where are you unsure about the state of your security practices?

STEP 4

Define the ISMS Scope

Action items:

- [ ] Determine your ISMS scope in terms of your organization's business functions, information processing systems, and information processing environments
- [ ] Determine which aspects of your business are in and out of scope
- [ ] Inform stakeholders of your ISMS scope
- [ ] Conduct a risk assessment
- [ ] Complete your statement of applicability (SoA)

STEP 5

Create and Implement an ISMS Plan

Action items:

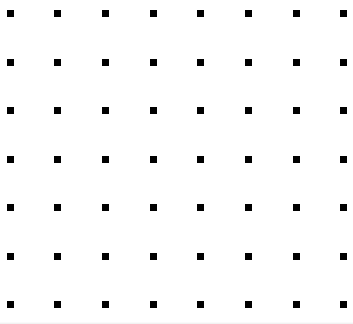
- [ ] Create a plan document that clearly defines the responsibilities and authority structures within your ISMS
- [ ] Document procedures and processes for handling various security incidents, including:
  - [ ] Managing access control
  - [ ] Confidentiality
  - [ ] Integrity
  - [ ] Availability of information assets
  - [ ] Incident response

STEP 6

Train Employees on Policies and Procedures

Action items:

- [ ] Train all team members on new ISMS policies and procedures
- [ ] Train relevant team members on your incident response plans
- [ ] Establish disciplinary or sanctions policies or processes for team members found out of compliance with mandatory infosec requirements



STEP 7

Conduct an Internal Audit

Action items:

- [ ] Secure a non-biased individual or group to examine your ISMS

> This can be conducted by an internal team that was not part of setting up and documenting your ISMS, or an independent external reviewer

- [ ] The internal auditor will:
  - [ ] Review all documentation
  - [ ] Review your ISMS
  - [ ] Conduct penetration testing
  - [ ] Collect evidence on what is and isn't working
- [ ] The auditor will produce an internal audit report that details corrective actions and recommendations, limitations, and other observations
- [ ] After you receive the report, work with your ISO 27001 team to address listed non-conformities

STEP 8

Find an Accredited Auditor to Lead the ISO 27001 Certification Audit

Action items:

- [ ] Find an accredited auditor to conduct your ISO 27001 Certification Audit
- [ ] Undergo a Stage 1 audit
- [ ] Obtain and address feedback from the Stage 1 audit
- [ ] Undergo a Stage 2 audit
- [ ] Address specific non-conformities identified by your auditor
- [ ] Receive ISO 27001 certification

How Drata Can Help You Clear the Path to ISO 27001 Certification

ISO 27001 certification can help you create better business outcomes, but it can be daunting to take on. Use this ISO 27001 checklist to guide your way.

If you want to reduce the complexity even further, Drata can streamline your journey to ISO 27001 certification and many other frameworks by eliminating hundreds of hours of manual work.

Schedule a demo to see how we can help.

DRATA