Delinea

ISO 27001 Checklist:
A streamlined path to certification

Achieving ISO 27001 certification is a major milestone for organizations looking to elevate their information security practices.

However, the road to certification can seem daunting without the right tools and guidance. That's where our ISO 27001 checklist comes in—designed to guide you step by step, from building your security foundation to achieving compliance and, ultimately, protecting your business from potential security threats.

Why ISO 27001 matters

ISO 27001 certification isn't just about ticking boxes. It's about ensuring the integrity, confidentiality, and availability of your organization's data. Gaining this certification demonstrates to stakeholders that your organization meets global best practices for information security. But let's be honest—the journey to ISO 27001 compliance has its challenges. Our checklist simplifies that process, helping you stay nimble and proactive every step of the way.

ISO 27001 compliance checklist overview

Ready to tackle ISO 27001 compliance head-on? Below are the essential steps to guide your organization from start to finish, ensuring your Information Security Management System (ISMS) is airtight and ready for audit.

Pro Tip: Download the compliance checklist to keep everything organized and on track.

Key steps to ISO 27001 Certification

1 Develop an implementation team and plan

To get started, assemble a team of key stakeholders from across departments, such as IT, HR, and legal. Define clear roles and responsibilities so that everyone knows what part they play in the certification process.

Action Items:

- ✓ Identify team members and assign responsibilities.
- ✓ Outline a project plan with milestones.

2 Understand ISO 27001 requirements

ISO 27001 includes detailed clauses and controls. It's crucial that your team understands Clauses 4–10 and Annex A, which lays out 114 security controls.

Action Items:

- ✓ Review and map out Clauses 4–10.
- ✓ Assign controls based on Annex A that apply to your organization.

3 Conduct a gap analysis

Where do you stand today? A gap analysis will help you identify where your current security policies fall short and what needs to be fixed to meet ISO 27001 standards.

Action Items:

- ✓ Perform a gap analysis on your existing ISMS.
- ✓ Prioritize action items based on identified gaps.

4 Define the ISMS scope

Determining the scope of your ISMS is vital. This ensures you're covering all critical assets while maintaining focus. Based on this, conduct a risk assessment and draft a Statement of Applicability (SoA).

Action Items:

- ✓ Define what systems, processes, and departments fall under your ISMS.
- ✓ Complete your risk assessment and prepare the SoA.

5 Create and implement ISMS policies and controls

Documentation is your best friend here. Create clear, actionable policies that everyone in your organization can understand and follow.

Action Items:

- Write comprehensive policies for ISMS, access controls, incident management, etc.
- Ensure policies reflect the requirements of ISO 27001.

6 Train employees on policies and procedures

People are your first line of defense. Ensure everyone knows what to do—and why—by implementing effective training programs.

Action Items:

- Develop a robust training schedule.
- Regularly test employees on security policies and incident response.

7 Conduct an internal audit

Before inviting external auditors, perform a thorough internal audit to catch any issues early. This will give you time to fix them before the official audit.

Action Items:

- Conduct an internal audit.
- Resolve any non-conformities identified.

8 Prepare documentation and evidence

Auditors love documentation. Gather all required paperwork, from your ISMS policies to your risk assessments and SoA. These documents will prove that your ISMS is built to ISO 27001 standards.

Action Items:

- Organize all relevant documents.
- Double-check that everything is accurate and up to date.

9 Conduct a Stage 1 audit

The Stage 1 audit is your first official step toward certification. Auditors will focus on your documentation to ensure your ISMS is designed correctly.

Action Items:

- Schedule your Stage 1 audit.
- Address any feedback or issues that arise.

10 Conduct a Stage 2 audit

In this final step, auditors will test your ISMS in action. They'll evaluate whether your security measures are effective and compliant with ISO 27001.

Action Items:

- Complete the Stage 2 audit.
- Tackle any final issues before certification is granted.

11 Plan for ongoing audits and surveillance

Certification doesn't end with the audit. To maintain ISO 27001 compliance, you must schedule regular surveillance audits and stay on top of any new requirements.

Action Items:

- Plan for future surveillance and recertification audits.
- Keep your ISMS updated to meet evolving security threats.

12 Commit to continuous improvement

Security is a moving target. ISO 27001 encourages continuous improvement, which means consistently monitoring and evolving your ISMS to meet new challenges.

Action Items:

- ✓ Set up a process for ongoing monitoring and improvements.
- ✓ Update your ISMS documentation and controls as needed.

13 Consider automation for ISO 27001 certification

Don't let the manual workload bog you down. Compliance automation tools can streamline your efforts, helping you stay agile while reducing the time and cost of managing compliance.

Action Items:

- ✓ Evaluate tools that automate ISMS monitoring, documentation, and audits.
- ✓ Integrate automation solutions to keep your certification on track.

Implementation tips for ISO 27001 success

- **Achieve executive buy-in:** Getting leadership on board is crucial for allocating resources and driving a security-first culture.
- **Document as you go:** Staying organized throughout the process will save you headaches later on.
- **Stay updated:** ISO 27001 requirements may change, so keep your team informed of the latest developments.
- **Adapt the scope:** Reevaluate the scope of your ISMS regularly to ensure it reflects your evolving business environment.

Tools and Support for ISO 27001 Certification

Compliance doesn't need to be complicated. **Platforms like Delinea** offer automation solutions that simplify the ISO 27001 certification process by centralizing controls, documentation, and audit preparation. These tools help you maintain compliance, reduce the manual workload, and stay ahead of any changes in the regulatory landscape.

Delinea

Delinea is a pioneer in securing identities through centralized authorization, making organizations more secure by seamlessly governing their interactions across modern enterprise. It applies context and intelligence throughout the identity lifecycle, across cloud and traditional infrastructure, data, and SaaS applications to eliminate identity-related threats. Delinea uniquely provides intelligent authorization for all identities, allowing precise user identification, appropriate access assignment, interaction monitoring, and swift response to irregularities. The Delinea Platform accelerates adoption and boosts productivity, deploying in weeks, not months, requiring just 10% of the resources compared to competitors. Discover more about Delinea on **delinea.com**, **LinkedIn**, **X**, and **YouTube**.