ISO 27001-Implementation Guide
Structured Certification – and Long-Term Security

Your concise overview of building a practical Information Security Management System (ISMS) – from the initial assessment to successful certification.

iso-easy
ISO 27001

ISO 27001 is not a project. It is a system.

ISO 27001 certification is not a one-time objective, but a structured process.

An effective Information Security Management System (ISMS) evolves alongside your company — just like your processes, your IT landscape, and your risks. New tools, new customer requirements, new regulatory obligations:

With every change, the responsibility for your information security grows.

That is why it is not just about passing an audit.
It is about building a lean, resilient system that works sustainably — without unnecessary bureaucracy.

iso-easy makes ISO 27001 realistically achievable for small and medium-sized enterprises.

Small and medium-sized companies in particular face specific challenges:

- Limited internal resources
- No dedicated ISO expert in-house
- Time pressure driven by customer requirements
- Uncertainty in interpreting the standard

This is where iso-easy comes in.

We develop a lean, audit-ready, and practical ISMS together with you — tailored to your organization, without corporate overhead and without unnecessary bureaucracy.

Clarity

You always know where you stand and what the next step is.

Pragmatism

We focus on what is truly relevant and audit-compliant.

Structure

A clear roadmap reduces effort, costs, and uncertainty.

iso-easy
ISO 27001

Your Path to ISO 27001 Certification

Every stage on the path to certification is essential — from the initial assessment to the internal audit as a rehearsal before the external audit.

iso-easy guides you through all phases:

PHASE 1:
Initial Assessment (Gap Analysis)

We systematically review where your company stands in comparison to ISO 27001. Existing processes are evaluated, gaps are identified and prioritized.

Result: Transparency regarding maturity level, required effort, and areas for action.

Why a Gap Analysis is essential:

- **Weaknesses become visible:**
  A gap analysis functions like a structured security check. It reliably identifies gaps and weaknesses within your existing security organization.
- **Requirements are systematically fulfilled:**
  Different industries are subject to different regulations. The gap analysis serves as guidance to ensure that all relevant requirements are met and that your organization remains up to date from a regulatory perspective.
- **Optimized resource and budget planning:**
  Early identification of necessary actions allows measures to be prioritized in a targeted manner. This creates planning reliability and enables more efficient use of budget and personnel.
- **Continuous relevance of your security structure:**
  A gap analysis is not a one-time activity, but a recurring quality check. It ensures that your information security remains effective in the long term and adapts to new developments.

iso-easy
ISO 27001

Your Path to ISO 27001 Certification

PHASE 2:
Define the Scope & Structure of the ISMS

Together, we define:

- Scope of application
- Responsibilities
- Security objectives
- Organizational framework conditions

This creates a solid foundation for your ISMS.

PHASE 3:
Systematic Identification of Risks and Assets

Identify information assets.
Assess threats.
Prioritize risks.
Based on this, we develop realistic and effective measures.

Why the systematic identification of assets and risks is essential:

- You know what needs to be protected — and from what:
  Through the structured identification of your information assets and the assessment of potential threats, you gain a comprehensive view of your security situation.
- Weaknesses and risks are identified at an early stage:
  The combined analysis reveals not only which assets are particularly critical, but also where concrete vulnerabilities or threats exist.
- Legal and regulatory requirements are fulfilled:
  Transparent asset and risk management supports you in systematically complying with legal and industry-specific requirements.
- Clear prioritization of actions:
  Not every risk is equally critical. Risk evaluation helps you prioritize measures effectively and allocate resources efficiently.
- Your organization remains resilient and capable of action:
  Understanding your information assets and actively managing risks reduces disruptions, prevents damage, and protects your long-term reputation and business operations.

Your Path to ISO 27001 Certification

PHASE 4:
Establish Policies & Documentation

ISO 27001 requires structured evidence. Together, we create:

- Security policies
- Process descriptions
- Statement of Applicability (SoA)
- Required supporting documentation

Audit-compliant. Clear. Practical.

Why structured documentation is indispensable:

- **It defines binding security standards:**
  Clear documentation establishes how your organization protects data, systems, and processes. It creates transparency regarding roles, responsibilities, and security measures.
- **It makes implementation traceable and manageable:**
  Documented processes serve as guidelines for the practical implementation of security controls — from access management to technical and organizational measures.
- **It ensures audit readiness and compliance:**
  ISO 27001 requires documented policies and procedures. Only well-structured documentation enables you to demonstrate conformity and prepare effectively for audits.

With iso-easy, you build on a proven foundation

iso-easy provides all necessary documents, templates, and proven methodologies as a shared basis.

Instead of starting from scratch, we work with a structured and field-tested documentation set that:

- Covers all ISO 27001 requirements
- Is designed to be audit-compliant
- Is tailored to your organization
- Remains clear and practical

The result is not an overloaded paper system, but a functioning ISMS that can be applied in daily operations.

iso-easy
ISO 27001

Your Path to ISO 27001 Certification

PHASE 5:
Training & Awareness

An ISMS only works if employees understand it. We support you with:

- Management briefings
- Employee awareness sessions
- Role clarification (e.g., Information Security Officer)
- Employee training in cooperation with our online training partner Perseus

Why this is crucial for ISO 27001 certification:

- Shared understanding of information security across the organization:
  All employees are familiar with the defined information security rules and follow consistent standards. This ensures that information security is not only documented but actively practiced in daily operations.
- Reduction of security risks:
  Trained and sensitized employees recognize potential threats at an early stage and respond appropriately. This significantly reduces the likelihood of security incidents.

PHASE 6:
Internal Audit & Management Review

The internal audit is your rehearsal.

We systematically verify whether your ISMS is compliant with the standard and audit-ready — and close any remaining gaps.

Why the internal audit is a key success factor:

- Identifying and resolving weaknesses early:
  The internal audit uncovers gaps and optimization potential within the ISMS before the external certification audit takes place. This allows corrective actions to be implemented without audit pressure.
- Confident preparation for the certification audit:
  Through structured internal review, you ensure that processes, documentation, and controls are implemented in compliance with the standard. This increases confidence during the external audit and significantly improves the likelihood of success.

iso-easy
ISO 27001

Your Path to ISO 27001 Certification

PHASE 7:
Support During the External Audit & Ensuring Sustainability

We guide you through the certification audit — both professionally and organizationally.

From coordinating with the certification body and preparing for the audit to structured support during the assessment itself, we stand by your side.

Objective:
A structured, confident audit — without surprises.

Achieving Certification — and Maintaining It
Compliance with ISO 27001 requirements does not end with a successful external audit.

Information security is an ongoing process.
New risks emerge. Processes evolve. Organizations grow.

Accordingly, your ISMS and security measures must be reviewed and adjusted on a regular basis.

We support you in:

- Systematically implementing audit findings
- Continuously updating risks and measures
- Keeping policies and documentation up to date
- Preparing confidently for surveillance audits

This ensures not only certification success,
but also the long-term effectiveness of your Information Security Management System.

iso-easy
ISO 27001

Staying Certified — Not Just Getting Certified

ISO 27001 certification is not an endpoint.
It marks the beginning of a continuous improvement process.

New risks arise.
Processes change.
Organizations grow.

An effective ISMS is regularly reviewed, adjusted, and further developed.

iso-easy also supports you after initial certification with:

- Updating the risk analysis
- Adjusting policies
- Preparing for surveillance audits
- Optional external Information Security Officer (ISO) services

What You Receive at the End

With iso-easy, you receive more than a certificate — you gain a robust system:

- ✓ Clearly defined ISMS scope
- ✓ Documented security objectives
- ✓ Comprehensive risk analysis
- ✓ Statement of Applicability
- ✓ Audit-ready documentation
- ✓ Internal audit report
- ✓ Management review documentation
- ✓ Structured framework for continuous improvement

iso-easy
ISO 27001

Why iso-easy?

NOTIVIA GmbH

iso-easy is part of Notivia GmbH. With more than 30 years of experience in web applications, IT security, compliance, and regulatory requirements for customers like Allianz, BMW, BAUHAUS, SAMSUNG, Zeiss, we bring extensive practical expertise to every project. Visit our website notivia.de.

Our focus is deliberately on:

- Small and medium-sized enterprises
- Pragmatic implementation
- Personal guidance instead of tool overload
- Clear communication at eye level

We do not see ISO 27001 as a pure documentation exercise,
but as a strategic building block for sustainable information security.

Your Journey to ISO 27001 Certification Starts Now

There is a lot to consider — we are aware of that.

With a structured approach and an experienced partner at your side, ISO 27001 becomes manageable and predictable.

If you would like to explore what your specific path could look like,
schedule a non-binding initial consultation with our experts.

Schedule your free initial consultation now
Implement ISO 27001 in a structured, lean, and audit-ready manner.

Phone: +49 711 35 15 705
Email: feedback@iso-easy.de

iso-easy
ISO 27001