Internal Audit according to ISO 27001

**Assess effectiveness. Identify gaps.
Ensure certification readiness.**

iso-easy
ISO 27001

Internal Audit according to ISO 27001

An effective ISMS is not defined by documentation — but by its real-world performance.

ISO 27001 explicitly requires organizations to conduct internal audits at planned intervals to determine whether the Information Security Management System:

- conforms to ISO 27001 requirements
- is effectively implemented
- is maintained and continuously improved

An internal audit is therefore not a formal checkbox.
It is a mandatory prerequisite for certification readiness.

And at the same time, it is your opportunity to identify weaknesses — before an external auditor does.

Why Internal Audits Are Often Underestimated

In practice, we frequently observe:

- Internal audits are scheduled too late
- Checklists are completed mechanically
- Audit methodology lacks structure
- Findings remain superficial
- Corrective actions are not systematically tracked
- Management reviews become purely formal

The result:

- Uncertainty during certification audits
- Unexpected nonconformities
- Time pressure before Stage 2
- Insufficient evidence of effectiveness

An internal audit is not a rehearsal.
It is a structured effectiveness test of your ISMS.

iso-easy
ISO 27001

The iso-easy Approach

We conduct internal audits the way certification bodies assess organizations.
Structured. Evidence-based. Practical.
The goal is not “pass or fail.”
The goal is clarity.

You receive:

✓ Transparent assessment of actual system maturity
✓ Clearly structured findings
✓ Concrete recommendations
✓ Prioritized corrective actions
✓ Audit-ready documentation

Our Audit Framework

1. System & Documentation Review

We evaluate, among others:

- Scope & context definition
- Risk management methodology
- Statement of Applicability
- Asset register
- Policy structure
- Supplier management
- Incident management
- Change management
- Awareness & training evidence

Not only for formal completeness —
but for consistency and real-world applicability.

iso-easy
ISO 27001

2. Effectiveness Assessment in Practice

An ISMS is only as strong as its implementation.

Therefore, we assess:

- Are roles and responsibilities clearly understood and lived?
- Are processes actually applied in daily operations?
- Is risk management embedded in decision-making?
- Are corrective actions tracked effectively?
- Is top management sufficiently involved?

This is where we determine whether the system truly works — or merely exists on paper.

3. Structured Audit Interviews

We conduct structured interviews with:

- Executive management
- IT leadership
- Operational departments
- Information Security Officers

The objective is to realistically evaluate awareness, implementation depth, and risk understanding.

This builds confidence — internally and externally.

Our Audit Framework

4. Comprehensive Audit Report

You receive a structured audit report including:

- Findings (Major / Minor / Observations)
- Risk assessment of deviations
- Prioritized action recommendations
- Implementation guidance
- Documentation improvement suggestions
- Preparation guidance for Stage 1 / Stage 2

The internal audit becomes a strategic decision-making tool — not just a compliance exercise.

Added Value Before Certification

A professionally conducted internal audit significantly reduces:

- Audit uncertainty
- Nonconformity risks
- Post-Stage 1 rework
- Reputational risk
- Project delays

It creates:

- Clarity
- Structure
- Management transparency
- Certification readiness

When Is the Right Time?

An internal audit is advisable:

- Before certification audits
- After significant organizational changes
- After major IT transitions
- Following security incidents
- When system maturity is unclear
- As part of the annual audit cycle

Recommended timing:
4–8 weeks before the external certification audit.

Internal vs. External Audit Execution

Many organizations ask:

Should we conduct the internal audit ourselves?

Theoretically: yes.
Practically: often challenging.

Typical challenges:

- Lack of independence
- Role conflicts
- Operational blind spots
- Limited time resources
- Insufficient audit methodology

An external auditor provides:
- Objectivity
- Certification body perspective
- Cross-project experience
- Methodological rigor
- Unbiased evaluation

Economic Perspective

An internal audit is not an additional burden — it is controlled risk mitigation.

Compared to potential certification audit deviations, it is a structured and predictable investment.

Typical scope:

1–3 audit days (depending on organizational size)
including audit report and corrective action guidance

Typical Timeline

Preparation: 1–2 weeks
Audit execution: 1–3 days
Report delivery: within a few working days

You gain clarity quickly — without disrupting your certification timeline.

Optional Extensions

- Management review facilitation
- Corrective action tracking support
- SoA optimization
- Risk methodology refinement
- Stage 1 / Stage 2 audit support

Working with iso-easy

iso-easy is part of Notivia GmbH, with over 30 years of experience in the digital sector, IT security, and compliance, serving clients such as BMW, Allianz, Zeiss, and SAMSUNG.
Simply visit notivia.de

Our internal audits are based on:

- Hands-on ISO implementation experience
- Certification audit exposure
- Technical expertise
- Regulatory knowledge
- Practical, business-oriented execution

We do not audit theoretically.
We audit with a certification-focused mindset.

Your Next Step

If you would like to understand how audit-ready your ISMS truly is, let's discuss:

- Your current maturity level
- Your certification timeline
- Your internal audit structure
- Your resource planning

A strong internal audit is not a formality.
It is your final confidence check before certification.

Schedule your free initial consultation now.

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