ISO 27001 Internes Audit

**Sicherheit überprüfen. Lücken erkennen.
Audit-Reife herstellen.**

iso-easy
ISO 27001

Internes Audit nach ISO 27001

Ein funktionierendes ISMS entsteht nicht durch Dokumente –
sondern durch Wirksamkeit.

Die ISO 27001 verlangt ausdrücklich:

Organisationen müssen in geplanten Abständen interne Audits durchführen, um zu bewerten, ob das Informationssicherheits-Managementsystem

- normkonform ist
- wirksam umgesetzt wird
- und kontinuierlich verbessert wird.

Das interne Audit ist damit kein optionaler Projektschritt.
Es ist die formale Voraussetzung für Zertifizierungsreife.

Und gleichzeitig die beste Gelegenheit, Schwächen zu erkennen – bevor es der externe Auditor tut.

Warum interne Audits oft unterschätzt werden

In der Praxis beobachten wir häufig:

Interne Audits werden zu spät geplant
Checklisten werden mechanisch abgearbeitet
Es fehlt methodische Auditstruktur
Feststellungen bleiben zu oberflächlich
Maßnahmen werden nicht konsequent verfolgt
Management-Reviews bleiben formal

Das Ergebnis:

Unsicherheit im Zertifizierungsaudit
Unerwartete Nebenabweichungen
Zeitdruck kurz vor Stage 2
Fehlende Nachweise zur Wirksamkeit

Ein internes Audit ist keine Simulation.
Es ist ein systematischer Wirksamkeitstest Ihres ISMS.

iso-easy
ISO 27001

Der Ansatz von iso-easy

Wir führen interne Audits so durch, wie externe Zertifizierer prüfen.
Strukturiert. Evidenzbasiert. Praxisnah.

Ziel ist nicht „Bestanden oder Nicht bestanden“. Ziel ist Klarheit.

Sie erhalten:

✓ Transparenz über tatsächliche Systemreife
✓ Nachvollziehbare Feststellungen
✓ Konkrete Handlungsempfehlungen
✓ Priorisierte Maßnahmen
✓ Audit-sichere Dokumentation

Unser Prüfmodell

1. System- & Dokumentenprüfung

Wir analysieren u. a.:

- Scope & Kontext
- Risikomanagement-Methodik
- Statement of Applicability
- Asset-Register
- Richtlinienstruktur
- Lieferantenbewertung
- Incident-Management
- Change-Prozesse
- Awareness-Nachweise

Nicht nur formal – sondern auf Konsistenz und Umsetzbarkeit.

iso-easy
ISO 27001

Unser Prüfmodell

2. Wirksamkeitsprüfung in der Praxis

Ein ISMS ist nur so gut wie seine Anwendung.

Deshalb prüfen wir:

- Sind Verantwortlichkeiten klar gelebt?
- Werden Prozesse tatsächlich angewendet?
- Ist das Risikomanagement im Alltag verankert?
- Werden Maßnahmen nachverfolgt?
- Ist das Management informiert und eingebunden?

Hier zeigt sich, ob das System trägt – oder nur dokumentiert ist.

3. Interviewbasierte Auditführung

Wir führen strukturierte Interviews mit:

- Geschäftsführung
- IT-Verantwortlichen
- Fachbereichen
- Informationssicherheitsbeauftragten

Ziel ist es,
Verständnis, Umsetzungstiefe und Risikobewusstsein realistisch zu bewerten.

Das schafft Sicherheit – intern wie extern.

Unser Prüfmodell

4. Auditbericht mit klarer Struktur

Sie erhalten einen vollständigen Auditbericht mit:

- Feststellungen (Major / Minor / Hinweise)
- Risikobewertung der Abweichungen
- Priorisierten Maßnahmenempfehlungen
- Umsetzungsempfehlungen
- Dokumentationshinweisen
- Vorbereitungshinweisen für Stage 1 / Stage 2

Damit wird das interne Audit zur konkreten Handlungsgrundlage.

Mehrwert vor dem Zertifizierungsaudit

Ein professionell durchgeführtes internes Audit reduziert:

- Audit-Unsicherheit
- Abweichungsrisiken
- Nacharbeit nach Stage 1
- Reputationsrisiken
- Zeitdruck im Projekt

Es schafft:

- Klarheit
- Struktur
- Management-Transparenz
- Zertifizierungsreife

Wann ist der richtige Zeitpunkt?

Ein internes Audit ist sinnvoll:

- Vor dem externen Zertifizierungsaudit
- Nach größeren organisatorischen Veränderungen
- Nach IT-Umstellungen
- Nach Sicherheitsvorfällen
- Bei Unsicherheit über Systemreife
- Als jährliche Pflichtprüfung

Empfehlung: 4–8 Wochen vor dem externen Audit.

Interne Ressourcen vs. Externe Durchführung

Viele Unternehmen stehen vor der Frage:

Soll das interne Audit selbst durchgeführt werden?

Theoretisch: Ja.
Praktisch: schwierig.

Herausforderungen bei interner Durchführung:

- Fehlende Objektivität
- Rollenkonflikte
- Betriebsblindheit
- Zeitmangel
- Fehlende Auditmethodik

Ein externer Auditor bringt:

- Unabhängigkeit
- Zertifizierer-Perspektive
- Praxisvergleich
- Erfahrung aus anderen Projekten
- Klare Bewertung ohne interne Interessenskonflikte

Wirtschaftliche Perspektive

Ein internes Audit ist kein Zusatzaufwand – es ist Risikominimierung.

Im Vergleich zu möglichen Abweichungen im Zertifizierungsaudit ist es eine kontrollierte, planbare Investition.

Typischer Rahmen:

1–3 Audittage (abhängig von Unternehmensgröße) inkl. Bericht & Maßnahmenempfehlung

Typische Projektdauer

Vorbereitung: 1–2 Wochen
Auditdurchführung: 1–3 Tage
Bericht: innerhalb weniger Werktage

Sie erhalten schnelle Klarheit – ohne Projektverzögerung.

Optional: Kombinierbar mit

- Management-Review-Moderation
- Maßnahmen-Tracking-Unterstützung
- SoA-Optimierung
- Risikomethodik-Review
- Audit-Begleitung bei Stage 1 / Stage 2

Zusammenarbeit mit iso-easy

iso-easy ist Teil der Notivia GmbH mit über 30 Jahren Erfahrung im Digitalbereich, in IT-Security und Compliance und betreut Kunden wie BMW, Allianz, Zeiss, SAMSUNG. Schauen Sie einfach vorbei notivia.de.

Wir verbinden:
- Technisches Verständnis
- Regulatorische Expertise
- Audit-Erfahrung
- Praxisorientierte Umsetzung

Unsere internen Audits basieren auf:
- Real durchgeführten ISO-Implementierungen
- Erfahrung aus Zertifizierungsaudits
- Technischem Verständnis
- Regulatorischer Expertise
- Praxisorientierter Umsetzung

Wir prüfen nicht theoretisch.
Wir prüfen mit Blick auf reale Zertifizierungssituationen.

Ihr nächster Schritt

Wenn Sie wissen möchten, wie audit-reif Ihr ISMS wirklich ist, sprechen wir unverbindlich über:

- Ihren aktuellen Stand
- Ihre geplante Zertifizierung
- Ihre interne Auditstruktur
- Ihre Zeitplanung

Ein starkes internes Audit ist kein Haken auf der To-do-Liste.
Es ist Ihr Sicherheitstest vor dem Ernstfall.

Jetzt kostenfreies Erstgespräch vereinbaren.

Telefon: +49 711 35 15 705
E-Mail: feedback@iso-easy.de