ISO 27001 Einführung

Vom Chaos zur auditfähigen Dokumentation

Pragmatische Einführung · Dokumentation durch SMCT MANAGEMENT · Klarer Weg zur Auditfähigkeit

SMCT MANAGEMENT

Ausgangslage: Viele Anforderungen, wenig Ordnung

Die Einführung scheitert selten am Willen – meistens fehlen Struktur, Nachweise und eine belastbare Dokumentation.

1

Typische Situation im Unternehmen

Informationen liegen verteilt in E-Mails, Ordnern, Tickets, Excel-Listen und Köpfen. Verantwortlichkeiten sind bekannt, aber selten eindeutig dokumentiert.

2

Risiken sind vorhanden, aber nicht bewertet

Server, Cloud-Dienste, Kundendaten, VPN, Notebooks, Backup und Dienstleister sind im Alltag wichtig. Für das Audit fehlen aber nachvollziehbare Bewertungen.

3

Nachweise werden zu spät gesammelt

Kurz vor dem Audit beginnt die Suche nach Screenshots, Protokollen, Richtlinien, Freigaben und Verträgen. Dadurch entsteht unnötiger Druck.

Ziel der Einführung ist nicht mehr Papier, sondern ein nachvollziehbares System: Wer macht was, welches Risiko besteht, welche Maßnahme ist umgesetzt und welcher Nachweis belegt dies?

Zielbild: Auditfähige Dokumentation statt Projektchaos

Auditfähig bedeutet: Anforderungen, Risiken, Maßnahmen und Nachweise sind sauber miteinander verbunden.

1 **Nachvollziehbar**

Jede Festlegung ist begründet: aus Normanforderung, Risiko, Vertrag, Kundenanforderung oder gesetzlicher Anforderung.

2 **Vollständig**

Pflichtdokumente, Prozesse, SoA, Risikobewertung, Rollen, Auditprogramm und Managementbewertung sind vorhanden.

3 **Praxisnah**

Die Dokumentation beschreibt die tatsächliche Arbeitsweise und bleibt für Geschäftsführung, IT und Mitarbeitende verständlich.

4 **Nachweisbar**

Technische und organisatorische Maßnahmen werden durch Screenshots, Protokolle, Verträge, Listen und Freigaben belegt.

ISO 27001 in einfachen Worten

Die Norm verlangt kein perfektes Unternehmen, sondern ein gesteuertes Informationssicherheits-Managementsystem.

1

Kontext & Anforderungen

Was ist intern und extern relevant? Welche Kunden-, gesetzlichen und vertraglichen Anforderungen bestehen?

2

Risiken & Chancen

Welche Informationen, Systeme und Dienstleistungen sind kritisch? Welche Risiken müssen behandelt werden?

3

Maßnahmen & Nachweise

Welche Sicherheitsmaßnahmen sind ausgewählt, umgesetzt, verantwortlich gemacht und nachweisbar?

4

Verbesserung

Interne Audits, Managementbewertung, Maßnahmenverfolgung und kontinuierliche Verbesserung halten das System lebendig.

Kernfrage im Audit: Kann das Unternehmen zeigen, dass Informationssicherheit geplant, umgesetzt, überprüft und verbessert wird?

Der Weg von Rohinformationen zur Auditfähigkeit

SMCT MANAGEMENT strukturiert die vorhandenen Informationen und erstellt daraus prüffähige Dokumente.

1

Informationen sammeln

Interviews, vorhandene Unterlagen, IT-Übersicht, Verträge, Tickets, Screenshots

2

Dokumentation erstellen

Richtlinien, Prozesse, Asset-Inventar, Risikoanalyse, SoA, Rollen, Ziele

3

Umsetzung steuern

Maßnahmenplan, Verantwortliche, Prioritäten, Fristen, Status und Restrisiko

4

Nachweise sichern

Screenshots, Protokolle, Schulungen, Verträge, Prüfberichte, Freigaben

5

Audit vorbereiten

Interner Audit, Managementbewertung, Korrekturen, Zertifizierungsgespräch

Wichtig: Der Kunde muss das Managementsystem nicht selbst „schreiben“. Er liefert fachliche Informationen, Entscheidungen und technische Nachweise. SMCT MANAGEMENT erstellt daraus die auditfähige Struktur.

Klare Arbeitsteilung: Kunde liefert, SMCT erstellt

So bleibt der interne Aufwand kalkulierbar und das Projekt kommt trotz Tagesgeschäft voran.

Kunde liefert	SMCT MANAGEMENT erstellt	Ergebnis für das Audit
Ansprechpartner, vorhandene Dokumente, technische Grundinformationen, Freigaben	Projektstruktur, Dokumentenlenkung, Rollenmodell, Interviewleitfäden, Maßnahmenplan	Klarer Projektstart mit nachvollziehbarer Aufgaben- und Entscheidungsstruktur
IT-Assets, Dienste, Standorte, Dienstleister, vorhandene Sicherheitsmaßnahmen	Asset-Inventar, Schutzbedarfsbewertung, Risikoanalyse, Risikobehandlungsplan	Risiken sind nicht nur bekannt, sondern bewertet, priorisiert und behandelt
Screenshots, Verträge, Systemauszüge, Schulungsnachweise, Protokolle	Nachweismappe, SoA-Verknüpfung, Auditvorbereitung, Managementbewertung	Auditor kann Anforderungen, Umsetzung und Nachweise schlüssig nachvollziehen

Der klassische Fehler: Der Kunde versucht alles selbst zu dokumentieren und verliert Zeit. Der pragmatische Weg: Informationen sammeln, Entscheidungen treffen, Dokumentation professionell aufbauen lassen.

Asset-Inventar: Die Grundlage jeder Risikoanalyse

Ohne belastbares Asset-Inventar fehlt die Verbindung zwischen Geschäft, IT, Risiken und Maßnahmen.

Asset	Bedeutung	Schutzbedarf	Typische Nachweise
ERP / Fachanwendung	Zentrale Geschäftsprozesse, Aufträge, Kundendaten, Abrechnung	Vertraulichkeit hoch Integrität hoch Verfügbarkeit hoch	Berechtigungskonzept, Backup, Patchstand, Rollenmodell
VPN / Remote-Zugang	Zugriff auf interne Systeme außerhalb des Standorts	Vertraulichkeit hoch Integrität mittel Verfügbarkeit mittel	MFA, VPN-Client-Anmeldung, Benutzerliste, Protokollierung
Cloud-Dienst / M365	E-Mail, Teams, SharePoint, Dokumente, Identitäten	Vertraulichkeit hoch Integrität hoch Verfügbarkeit mittel	Admin-Einstellungen, MFA, Conditional Access, Vertragsnachweise
IT-Dienstleister	Wartung, Administration, Backup, Support, Notfallhilfe	Abhängig von Zugriff und Kritikalität	Vertrag, AVV, Vertraulichkeit, Zugriffsregelung, SLA

Praxisregel Ein Asset ist nur auditfest, wenn Bedeutung, Verantwortlichkeit, Schutzbedarf, Risiken und Nachweise nachvollziehbar dokumentiert sind.

Risikobewertung und Risikobehandlung

Risiken werden nicht nur genannt, sondern bewertet, behandelt und mit Restrisiko dokumentiert.

1

1. Risiko beschreiben

Beispiel: Unbefugter Zugriff auf Kundendaten über kompromittierte VPN-Zugänge oder schwache Benutzerkonten.

2

2. Eintritt und Schaden bewerten

Bewertung z. B. Eintrittswahrscheinlichkeit × Schadensausmaß. Die Methode muss einfach, nachvollziehbar und wiederholbar sein.

3

3. Maßnahme festlegen

MFA, Benutzerprüfung, VPN-Protokollierung, Rollenfreigabe, regelmäßige Rezertifizierung und dokumentierte Verantwortlichkeit.

Beispiel	Vorher	Maßnahme	Nachher / Restrisiko
VPN-Zugriff	E 3 × S 3 = 9 Risiko hoch	MFA verpflichtend, Benutzerliste bereinigen, Zugriff protokollieren	E 2 × S 2 = 4 Restrisiko akzeptabel
Backup	E 2 × S 4 = 8 Risiko erhöht	Backup-Job überwachen, Restore-Test dokumentieren, getrennte Sicherung	E 1 × S 3 = 3 Restrisiko akzeptabel
Patchmanagement	E 3 × S 3 = 9 Risiko hoch	Patchzyklus, Verantwortliche, Ausnahmen und Tickets dokumentieren	E 2 × S 2 = 4 Restrisiko akzeptabel

Auditfrage: Ist erkennbar, warum eine Maßnahme ausgewählt wurde und wie sie das Risiko reduziert?

Statement of Applicability: Die Brücke zwischen Norm und Praxis

Die SoA zeigt, welche Annex-A-Maßnahmen relevant sind, warum sie gelten und wie sie umgesetzt werden.

1

Control auswählen

z. B. Zugriffskontrolle, Backup, Schwachstellenmanagement, Lieferantensteuerung

2

Relevanz begründen

anwendbar wegen Risiko, Kunde, Vertrag, gesetzlicher Anforderung oder Geschäftsprozess

3

Umsetzung beschreiben

konkrete organisatorische oder technische Maßnahme im Unternehmen

4

Nachweis zuordnen

Richtlinie, Screenshot, Protokoll, Vertrag, Ticket, Schulungsnachweis oder Freigabe

SoA-Feld	Auditfester Inhalt
Anwendbarkeit	Ja / Nein mit Begründung, nicht nur Häkchen
Umsetzungsstatus	umgesetzt, teilweise umgesetzt, geplant, nicht anwendbar
Verknüpfung	Risiko, Asset, Prozess, Richtlinie und Nachweis müssen zusammenpassen

Richtlinien und Prozesse: Nicht für den Ordner, sondern für den Betrieb

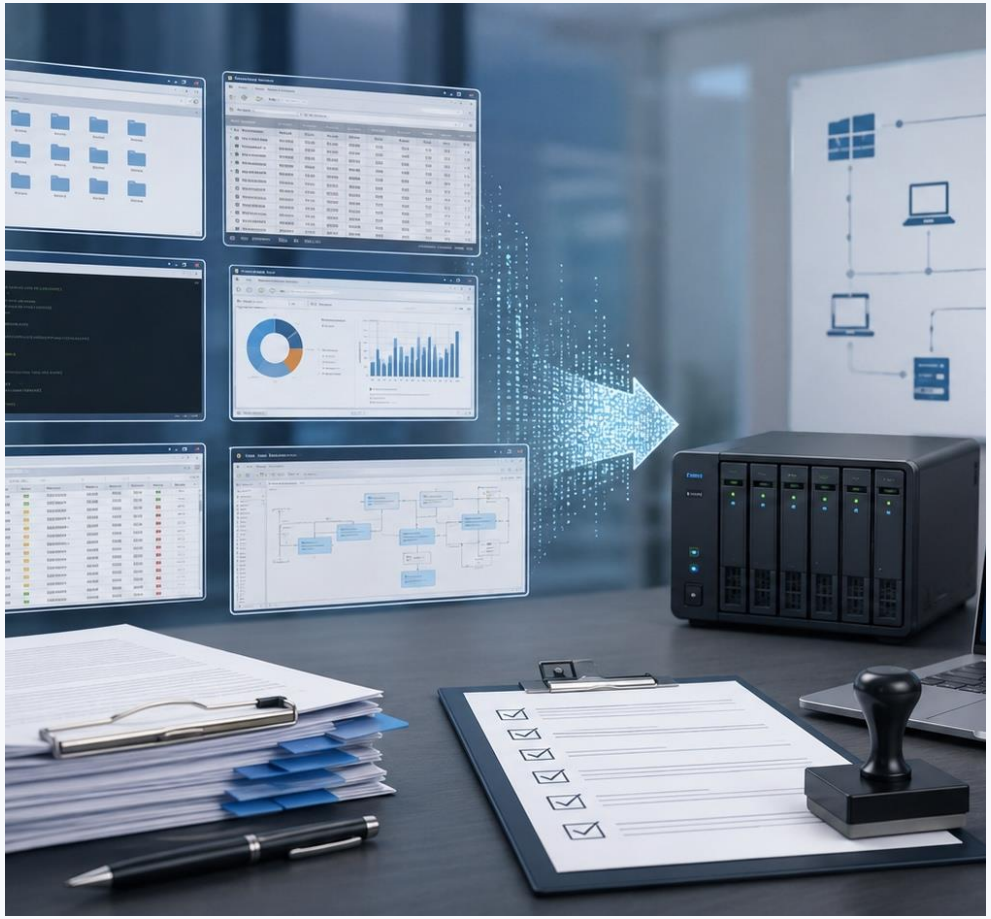
Gute Dokumentation beschreibt die tatsächliche Arbeitsweise und gibt klare Mindestregeln vor.

Dokument / Prozess	Zweck	Typischer Nachweis
Informationssicherheitsleitlinie	Verbindliche Grundausrichtung, Ziele und Verantwortlichkeiten der Geschäftsführung	Freigabe, Veröffentlichung, Schulungsnachweis
Zugriffs- und Berechtigungskonzept	Regeln für Benutzeranlage, Rollen, Rechteprüfung, Austritt und externe Zugriffe	Benutzerliste, Rollenmatrix, Rezertifizierung
Backup- und Wiederherstellungskonzept	Sicherung, Aufbewahrung, Trennung, Verantwortlichkeit und Restore-Test	Backup-Protokolle, Restore-Test, Monitoring
Incident-Management	Erkennung, Meldung, Bewertung, Eskalation, Dokumentation und Lessons Learned	Ticket, Vorfallbericht, Maßnahmenstatus
Lieferantensteuerung	Bewertung kritischer Dienstleister und vertragliche Absicherung von Sicherheitsanforderungen	Lieferantenliste, Vertrag, AVV, SLA, Prüfung

Pragmatischer Grundsatz: Lieber wenige, klare und gelebte Dokumente als viele theoretische Vorgaben ohne Bezug zum Betrieb.

Technische Nachweise: Was Auditoren typischerweise sehen wollen

Die Norm bewertet nicht nur Dokumente. Entscheidend ist, dass Sicherheitsmaßnahmen nachweisbar umgesetzt sind.



Thema	Möglicher Nachweis
Netzwerk / VLAN	VLAN-Strukturplan, Firewall-Regeln, Trennung von Servern, Clients, Gästen und Verwaltung
VPN / Remote-Arbeit	VPN-Client-Anmeldung, MFA, Benutzerliste, Homeoffice-Regeln, Freigabeprozess
Backup	Backup-Server, Backup-Clients, Protokolle, getrennte Sicherung, Wiederherstellungstest
Patchmanagement	Patchstatus, Ticket, Wartungsfenster, Ausnahmen, Verantwortlicher
Endpoint Protection	Defender/EDR-Status, Schadsoftwareprüfung, BitLocker, Gerätekonformität
Schwachstellen	Scanbericht, Risikobewertung, Ticket, Maßnahme, Frist, Abschlussnachweis

SMCT MANAGEMENT kann aus vorhandenen Systeminformationen eine geordnete Nachweismappe für Zertifizierungs- und Überwachungsaudits erstellen.

Rollen, Verantwortlichkeiten und Awareness

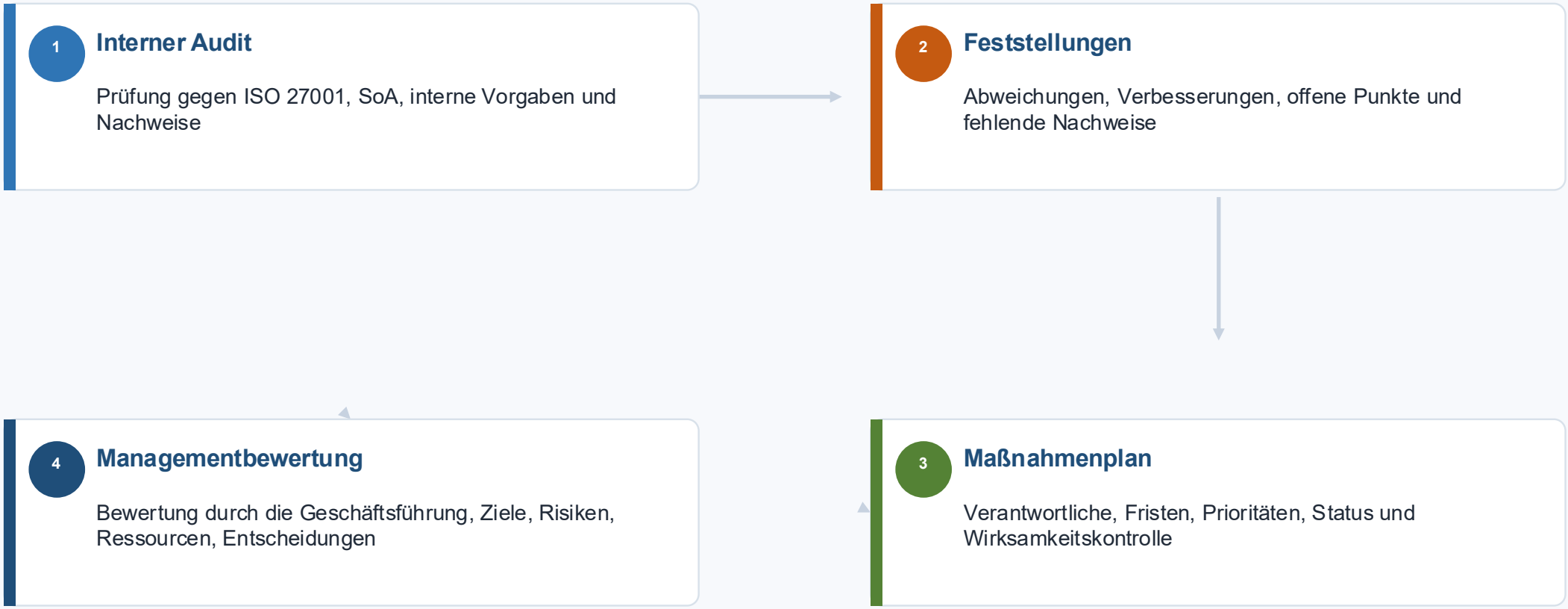
Informationssicherheit funktioniert nur, wenn Zuständigkeiten klar geregelt und Mitarbeitende sensibilisiert sind.

Rolle	Aufgabe	Nachweis
Geschäftsführung	Leitlinie freigeben, Ziele festlegen, Risiken akzeptieren, Ressourcen bereitstellen	Freigabe, Managementbewertung, Risikobeschluss
ISB / Verantwortlicher ISMS	System steuern, Dokumentation pflegen, Maßnahmen verfolgen, Audits koordinieren	Bestellung, Aufgabenbeschreibung, Maßnahmenstatus
IT-Verantwortliche	Technische Maßnahmen umsetzen, Nachweise liefern, Schwachstellen behandeln	Tickets, Protokolle, Screenshots, Change-Nachweise
Mitarbeitende	Regeln einhalten, Vorfälle melden, sicher mit Informationen arbeiten	Unterweisung, Awareness-Test, Richtlinienbestätigung
Externe Dienstleister	Vertraulichkeit, sichere Administration, Support und definierte Serviceleistung	Vertrag, AVV, NDA, SLA, Zugriffsliste

RACI-Kurzlogik	Bedeutung im Projekt
R – Responsible	wer erledigt die Aufgabe operativ
A – Accountable	wer trifft die Entscheidung und trägt Verantwortung
C – Consulted	wer fachlich eingebunden wird
I – Informed	wer informiert werden muss

Interner Audit und Managementbewertung

Vor dem Zertifizierungsaudit wird geprüft, ob das System vollständig, wirksam und entscheidungsreif ist.



Der interne Audit ist kein Selbstzweck. Er ist die letzte systematische Kontrolle, bevor der Kunde gegenüber dem Zertifizierer belastbar auftreten muss.

Einführungsfahrplan: Realistisch, überschaubar, auditnah

Der genaue Zeitplan hängt von Unternehmensgröße, IT-Komplexität und vorhandener Dokumentation ab.

Woche 1–2	Woche 3–4	Woche 5–6	Woche 7–8	Woche 9–12
Start & Aufnahme	**Assets & Risiken**	**Dokumentation**	**Umsetzung & Nachweise**	**Auditvorbereitung**
Scope, Ansprechpartner, vorhandene Dokumente, IT-Übersicht, Projektplan	Asset-Inventar, Schutzbedarf, Risikoanalyse, erste Maßnahmenliste	Leitlinie, Prozesse, Rollen, Lieferanten, SoA, Nachweisstruktur	Technische Nachweise, offene Maßnahmen, Schulung, Freigaben	Interner Audit, Managementbewertung, Korrekturen, Zertifizierungsreife

Vorausschauend planen: Kritische Punkte sind meist technische Nachweise, Rollenfreigaben, Dienstleisterverträge, offene Maßnahmen und Managemententscheidungen.

Nächste Schritte im Erstgespräch

Ziel ist ein schneller, belastbarer Überblick: Was ist vorhanden, was fehlt und wie wird Auditfähigkeit erreicht?

1

1. Scope und Ziel klären

Welche Standorte, Systeme, Dienstleistungen, Kundenanforderungen und Zertifizierungsziele sollen abgedeckt werden?

2

2. Vorhandene Unterlagen sichten

Richtlinien, IT-Dokumentation, Verträge, Prozessbeschreibungen, Datenschutzunterlagen und bestehende Nachweise prüfen.

3

3. GAP und Aufwand bewerten

Fehlende Dokumente, technische Nachweise, Rollen, Risiken und offene Maßnahmen werden strukturiert ermittelt.

4

4. Projektplan festlegen

SMCT MANAGEMENT erstellt Dokumentation, Risikobewertung, SoA, Auditvorbereitung und unterstützt bis zur Zertifizierungsreife.

Kernaussage: Der Kunde bleibt im Tagesgeschäft handlungsfähig – SMCT MANAGEMENT führt Struktur, Dokumentation und Auditvorbereitung zusammen.