SECJUR

ISO/IEC 27001 für den Mittelstand

Der praktische Fahrplan für Founder und CEOs — von der Bestandsaufnahme bis zum Zertifikat.

Informationssicherheit ist im Mittelstand längst kein reines IT-Thema mehr. Ob Lieferantenbewertungen großer Konzerne, NIS-2-Pflichten oder Cyberversicherungs-Anforderungen — immer mehr Geschäftsentscheidungen hängen davon ab, wie ein Unternehmen seine Informationssicherheit strukturiert und nachweist. **ISO/IEC 27001** ist der international anerkannte Standard dafür — und liefert den Rahmen, um sensible Daten, Prozesse und Lieferantenbeziehungen **nachweisbar abzusichern.**

Wann ISO 27001 für mittelständische Unternehmen konkret wird:

TREIBER 01

Lieferketten-Compliance

Große Auftraggeber verlangen nachweisbare Informationssicherheit von ihren Lieferanten. Wer kein Zertifikat vorweisen kann, scheidet oft in der Vorqualifizierung aus — bevor das eigentliche Gespräch beginnt.

TREIBER 02

NIS-2 & gesetzliche Pflicht

Mit dem NIS2UmsuCG werden tausende Mittelständler als wichtige Einrichtungen eingestuft. ISO 27001 liefert das Rahmenwerk, um diese gesetzlichen Pflichten strukturiert und prüffest zu erfüllen.

TREIBER 03

Cyberversicherung & Risiko

Versicherer bewerten Sicherheitsreife zunehmend bei Prämien und Deckungsumfang. Ein ISMS nach ISO 27001 dokumentiert umgesetzte Kontrollen und reduziert das Schadenrisiko nachweisbar.

TREIBER 04

Wettbewerbsvorteil

Das Zertifikat ersetzt Dutzende individuelle Sicherheitsfragebögen und beschleunigt das Onboarding bei Enterprise-Auftraggebern erheblich — ein messbarer Vorsprung gegenüber nicht-zertifizierten Wettbewerbern.

Sicherheit als Wettbewerbsvorteil — messbar und nachweisbar

3–6 Monate

typische Umsetzungszeit mit Plattform & Expert:innen statt 12+ Monate im Eigenbau

Ein Nachweis

ersetzt unzählige Kunden-Fragebögen und beschleunigt Enterprise-Onboardings spürbar

93 Controls

strukturiert in vier Themenbereiche — als vollständiger Sicherheitsrahmen für IT & Daten

SECJUR

Ihr Weg zum ISMS — Schritt 1 bis 6

Die ersten sechs Schritte schaffen das Fundament: Auftrag, Geltungsbereich, Asset-Transparenz und eine belastbare Risikobeurteilung.

SCHRITT 01

Management-Sponsorship sichern

- [ ] Geschäftsführung formell als Sponsor des ISMS-Projekts gewinnen
- [ ] Budget, Ressourcen und Verantwortlichkeiten gemeinsam beschließen
- [ ] CISO oder Informationssicherheitsbeauftragte/n benennen
- [ ] Informationssicherheits-Richtlinie unterzeichnen und kommunizieren
- [ ] Projektzeitplan und Meilensteine mit dem Management abstimmen

SCHRITT 02

Geltungsbereich definieren

- [ ] Standorte, Systeme und Kernprozesse im ISMS-Scope festlegen
- [ ] Scope-Dokument erstellen und vom Management formell freigeben
- [ ] Schnittstellen zu Lieferanten und externen Partnern abgrenzen
- [ ] Regulatorische Anforderungen aus NIS-2 und DSGVO einbeziehen
- [ ] Ausschlüsse begründen und im Statement of Applicability dokumentieren

SCHRITT 03

Asset-Register aufbauen

- [ ] Alle Informationswerte inventarisieren: IT, Daten, Prozesse, Räumlichkeiten
- [ ] Asset-Owner für jeden einzelnen Wert benennen und in DCO hinterlegen
- [ ] Schutzbedarf klassifizieren: normal / hoch / sehr hoch je Wert
- [ ] Kritische Geschäftsprozesse und ihre technischen Abhängigkeiten dokumentieren
- [ ] Asset-Register regelmäßig gemeinsam aktualisieren und reviewen

SCHRITT 04

Risiken identifizieren und bewerten

- [ ] Risikobeurteilungsmethodik festlegen und schriftlich dokumentieren
- [ ] Bedrohungen und Schwachstellen je Asset systematisch identifizieren
- [ ] Eintrittswahrscheinlichkeit und Auswirkung je Risiko bewerten
- [ ] Risikoakzeptanzkriterien mit der Geschäftsführung gemeinsam vereinbaren
- [ ] Risikoregister in DCO anlegen, laufend aktuell halten und versionieren

SCHRITT 05

Maßnahmen wählen (SoA)

- [ ] Controls aus Anhang A (93 Maßnahmen) auswählen und einzeln begründen
- [ ] Statement of Applicability erstellen, versionieren und laufend pflegen
- [ ] Risikobehandlungsplan mit Verantwortlichen und verbindlichen Fristen aufsetzen
- [ ] Restrisiken formell durch die Geschäftsführung akzeptieren lassen
- [ ] Umsetzungsstatus der Controls kontinuierlich in DCO nachverfolgen

SCHRITT 06

Richtlinien und Lieferanten

- [ ] Kritische Lieferanten identifizieren und Sicherheitsanforderungen schriftlich vereinbaren
- [ ] ISMS-Kernrichtlinien erstellen: Zugriff, Klassifizierung, Incident-Response
- [ ] Dokumentenlenkung, Versionierung und Freigabeprozess im ISMS einrichten
- [ ] AVVs und Sicherheitsklauseln für alle genutzten Cloud-Dienste prüfen
- [ ] Lieferantenbewertungsprozess verankern und kalendarisch einplanen

SECJUR

Ihr Weg zum ISMS — Schritt 7 bis 12

Technische Maßnahmen umsetzen, intern prüfen und das Zertifizierungsaudit erfolgreich bestehen.

SCHRITT 07

Technische Controls umsetzen

- [ ] Zugriffskontrollen, MFA und Netzwerksegmentierung einführen
- [ ] Patch-Management und regelmäßiges Schwachstellen-Scanning etablieren
- [ ] Verschlüsselung für Daten in Ruhe und bei Übertragung umsetzen
- [ ] Logging und Monitoring für alle sicherheitsrelevanten Systeme einrichten
- [ ] Konfigurationsmanagement und Hardening-Standards für Server definieren

SCHRITT 08

Lieferkette absichern

- [ ] Regelmäßige Lieferantenbewertung als wiederkehrenden ISMS-Prozess verankern
- [ ] Sicherheitsanforderungen verbindlich in neue Lieferantenverträge aufnehmen
- [ ] Exit-Prozesse, Datenzurückgabe und Löschpflichten mit Dienstleistern klar regeln
- [ ] Kritische Abhängigkeiten von Einzellieferanten identifizieren und adressieren
- [ ] AVVs und Sicherheitsklauseln für alle Cloud-Dienste regelmäßig aktualisieren

SCHRITT 09

Awareness und Notfallvorsorge

- [ ] Pflichtschulungen und Awareness-Kampagnen für alle Mitarbeitenden durchführen
- [ ] Rollenspezifische Trainings und Phishing-Simulationen regelmäßig einplanen
- [ ] Incident-Response-Prozess vollständig dokumentieren, testen und üben
- [ ] Business-Continuity-Plan für alle kritischen Geschäftsprozesse entwickeln
- [ ] Meldeketten für Datenpannen nach DSGVO Art. 33 und NIS-2 verbindlich festlegen

SCHRITT 10

Internes Audit durchführen

- [ ] Internen Auditor benennen oder qualifizierten externen Auditor beauftragen
- [ ] Alle ISMS-Prozesse, Richtlinien und Controls systematisch auditieren
- [ ] Nichtkonformitäten und Verbesserungspotenziale vollständig dokumentieren
- [ ] Korrekturmaßnahmen mit klaren Verantwortlichen und verbindlichen Fristen einleiten
- [ ] Management Review auf Basis der Audit-Ergebnisse vorbereiten und durchführen

SCHRITT 11

Zertifizierungsaudit bestehen

- [ ] Akkreditierte Zertifizierungsstelle nach aktueller DAkkS-Liste auswählen
- [ ] Stage-1-Audit: Dokumentenprüfung gründlich vorbereiten und erfolgreich bestehen
- [ ] Stage-2-Audit: Wirksamkeitsprüfung vor Ort vollständig absolvieren
- [ ] Verbliebene Minor-Nichtkonformitäten fristgerecht schließen und nachweisen
- [ ] Zertifikat erhalten und Drei-Jahres-Zyklus für Überwachungsaudits einrichten

SCHRITT 12 — DAUERHAFT

ISMS langfristig betreiben

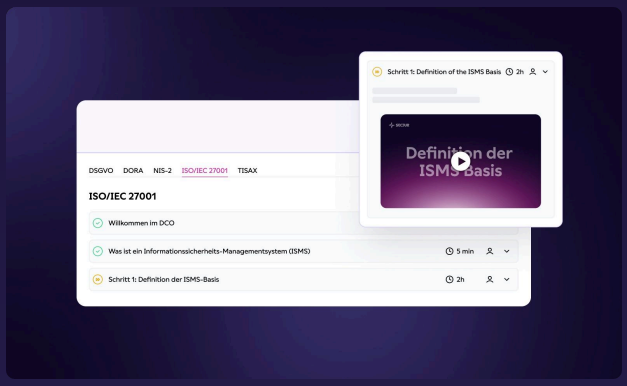
- [ ] Jährliche Überwachungsaudits und Re-Zertifizierung (alle 3 Jahre) fest einplanen
- [ ] Kontinuierlichen Verbesserungsprozess (KVP) strukturell im ISMS verankern
- [ ] Änderungen in Scope, Risiken und Controls laufend nachpflegen und versionieren
- [ ] Lessons Learned aus Sicherheitsvorfällen systematisch einarbeiten und teilen
- [ ] ISMS-Reifegrad jährlich messen und daraus konkrete Verbesserungsziele ableiten

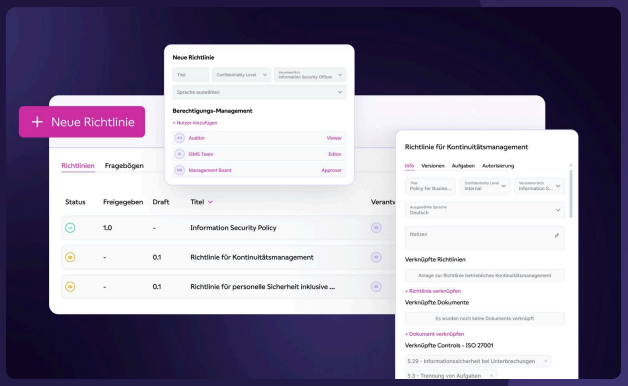
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

Mit der **SECJUR Automatisierungsplattform** und unseren **TÜV-zertifizierten Expert:innen** setzen Sie ISO 27001 in Rekordzeit um:

- Automatisierte Erstellung und Verwaltung Ihres ISMS
- Integriertes Risikomanagement & Lieferantenbewertungen
- Audit-Readiness auf Knopfdruck

Damit sparen Sie hunderte Stunden Aufwand – und sichern sich den entscheidenden Wettbewerbsvorteil bei großen Kundenprojekten.





Mit SECJUR zur automatisierten Compliance

"Mit SECJUR lassen sich alle NIS2-Anforderungen auf einer Plattform umsetzen. Dadurch konnten wir binnen einer Woche ein zentrales, skalierbares Richtliniensystem für die NIS2"

Dipl. Ing. Michael Dohr
Manager IT Security

Nordzucker

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR

MESSER Gases for Life · Nordzucker · PETER KÖLLN · SWT STAHLWERK THÜRINGEN · FEDDERSEN GRUPPE · oetinger aluminium

www.secjur.com