SECJUR

# ISO/IEC 27001 für Scaleups

Die Checkliste für Founder & CEOs — in 11 Schritten zur Zertifizierung.

Für Scaleups ist Informationssicherheit kein abstraktes Compliance-Thema — sie ist ein **direkter Umsatzhebel.** Enterprise-Kunden verlangen Sicherheitsnachweise, bevor Verträge unterschrieben werden. Investoren prüfen das ISMS in der Due Diligence. Acquirer berechnen offene Lücken in den Kaufpreis ein. **ISO/IEC 27001** ist der Standard, der diese Gespräche entscheidet — und in 3 bis 6 Monaten erreichbar.

## In diesen vier Situationen wird ISO 27001 für Scaleups kritisch:

ENTERPRISE SALES

### Vendor Assessments gewinnen

- ISO 27001 als Türöffner bei Enterprise-Deals
- Zertifikat ersetzt Dutzende Fragebögen
- Security-Reviews messbar beschleunigen
- Ausschluss in der Vorqualifizierung vermeiden

FUNDRAISING

### Tech Due Diligence bestehen

- Investoren prüfen Datensicherheit in Series B/C
- ISMS reduziert rote Flaggen im Investment-Prozess
- Schwächen bei Zugriffskontrollen kosten Bewertung
- Zertifikat signalisiert Reife und Stabilität

SKALIERUNG

### Sicherheit mitwachsen lassen

- Mit jedem Mitarbeitenden wächst die Angriffsfläche
- ISMS schafft klare Verantwortlichkeiten
- Sicherheitsprozesse skalieren mit dem Team
- Grundlage für NIS2- und DSGVO-Compliance

M&A & EXIT

### Bewertung schützen

- Käufer bewerten ISMS-Lücken als Haftungsrisiko
- Offene Findings führen zu Abschlägen
- Zertifikat ermöglicht saubere Due Diligence
- Nachverhandlungsrisiko bei Exit reduzieren

### 3-6 Monate

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

### 93 Controls

ISO 27001:2022 — alle automatisiert nachweisbar über ein Dashboard

### 1 Zertifikat

ersetzt unzählige Vendor-Fragebögen und beschleunigt das Onboarding

SECJUR

# Ihr Weg zum ISMS — Schritt 1 bis 6

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

SCHRITT 01

## Management-Commitment

- [ ] **Projekt** durch die Geschäftsführung formal beauftragen und dokumentieren
- [ ] **ISB** benennen und mit Mandat sowie ausreichend Budget ausstatten
- [ ] **Ressourcen,** Zeitplan und Verantwortlichkeiten durch GF freigeben
- [ ] **Projektziel,** Meilensteine und Risiken an das Team kommunizieren
- [ ] **Reporting-Rhythmus** und Eskalationswege mit der GF festlegen

SCHRITT 02

## Geltungsbereich definieren

- [ ] **Anwendungsbereich** des ISMS schriftlich dokumentieren und abstimmen
- [ ] **Standorte,** Abteilungen und relevante IT-Systeme vollständig erfassen
- [ ] **Schnittstellen** zu Partnern und bewusste Ausschlüsse klar abgrenzen
- [ ] **Scope-Dokument** durch die Geschäftsführung formell genehmigen lassen
- [ ] **Abhängigkeiten** zu externen Systemen und Dienstleistern klären

SCHRITT 03

## Asset-Register aufbauen

- [ ] **IT-Systeme,** Server und Endgeräte vollständig erfassen
- [ ] **Maschinen** und vernetzte Anlagen klassifizieren
- [ ] **Asset-Owner** und Schutzbedarf je Asset dokumentieren
- [ ] **Klassifizierungsschema** für Informationen definieren
- [ ] **Asset-Register** als lebendes Dokument etablieren

SCHRITT 04

## Risiken bewerten

- [ ] **Bewertungsmethode** und Risikoskala festlegen
- [ ] **Bedrohungen** und Schwachstellen je Asset identifizieren
- [ ] **Risikoakzeptanz** mit der Geschäftsführung abstimmen
- [ ] **Behandlungsplan** erstellen und priorisieren
- [ ] **Restrisiken** dokumentieren und freigeben lassen

SCHRITT 05

## Maßnahmen festlegen (SoA)

- [ ] **Controls** alle 93 auf Anwendbarkeit prüfen
- [ ] **SoA** erstellen: anwendbare Controls begründen
- [ ] **Ausschlüsse** nachvollziehbar dokumentieren
- [ ] **Genehmigung** der SoA durch Geschäftsführung einholen
- [ ] **Verantwortliche** und Budget je Control zuordnen

SCHRITT 06

## Leitlinien & Richtlinien

- [ ] **IS-Leitlinie** mit Schutzzielen schriftlich formulieren
- [ ] **Schutzziele** definieren: Vertraulichkeit, Integrität, Verfügbarkeit
- [ ] **Geltungsbereich** und Verantwortlichkeiten benennen
- [ ] **Geschäftsführung** unterzeichnet die Leitlinie formell
- [ ] **Kommunikation** an alle Mitarbeitenden sicherstellen

SECJUR

# Ihr Weg zum ISMS — Schritt 7 bis 11

Die zweite Hälfte bringt das ISMS in den Betrieb: technische Härtung, Notfallvorsorge, interne Prüfung, Zertifizierung.

SCHRITT 07

## Technische Maßnahmen

- [ ] **Netzwerke** segmentieren und IT/OT-Trennung einrichten
- [ ] **Patch-Management** für alle Systeme einführen
- [ ] **Backups** und Wiederherstellung regelmäßig testen
- [ ] **Zugriffsrechte** nach Need-to-know-Prinzip vergeben
- [ ] **Monitoring** und Logging für kritische Systeme einrichten

SCHRITT 08

## Lieferkette absichern

- [ ] **Dienstleister** und Partner nach Kritikalität bewerten
- [ ] **Sicherheitsanforderungen** vertraglich verankern (AVV)
- [ ] **Fernwartungszugänge** kontrollieren und protokollieren
- [ ] **Datenaustausch** mit OEMs und Partnern absichern
- [ ] **Lieferanten** jährlich neu bewerten und dokumentieren

SCHRITT 09

## Awareness & Notfallvorsorge

- [ ] **Schulungen** zu Cyberrisiken für alle Mitarbeitenden
- [ ] **Incident-Response-Plan** dokumentieren und erproben
- [ ] **Meldewege** für Sicherheitsvorfälle festlegen (NIS2)
- [ ] **Notfallübungen** für kritische Produktionsausfälle durchführen
- [ ] **Phishing-Tests** und Awareness-Kampagnen regelmäßig einplanen

SCHRITT 10

## Internes Audit & Review

- [ ] **Internes Audit** nach ISO 19011 planen und beauftragen
- [ ] **Non-Conformities** erfassen und Korrekturmaßnahmen einleiten
- [ ] **Managementbewertung** mit der Geschäftsführung durchführen
- [ ] **Wirksamkeit** aller implementierten Controls prüfen
- [ ] **KPIs** zur Informationssicherheit messen und berichten

SCHRITT 11

## Zertifizierungsaudit

- [ ] **Zertifizierungsstelle** (DAkkS-akkreditiert) auswählen
- [ ] **Stage-1-Audit** (Dokumentationsprüfung) vorbereiten
- [ ] **Stage-2-Audit** (Umsetzung vor Ort) erfolgreich bestehen
- [ ] **Zertifikat** erhalten, kommunizieren und vermarkten
- [ ] **Überwachungsaudits** jährlich einplanen und bestehen

FOUNDER-TIPP

## ISMS am Leben halten

- [ ] **KVP** — kontinuierliche Verbesserung im ISMS verankern
- [ ] **Überwachungsaudits** und Re-Zertifizierung vorausplanen
- [ ] **Neue Systeme** direkt ins Asset-Register aufnehmen
- [ ] **DCO-Plattform** statt Excel für ISMS-Pflege nutzen
- [ ] **Kennzahlen** regelmäßig an die Geschäftsführung berichten

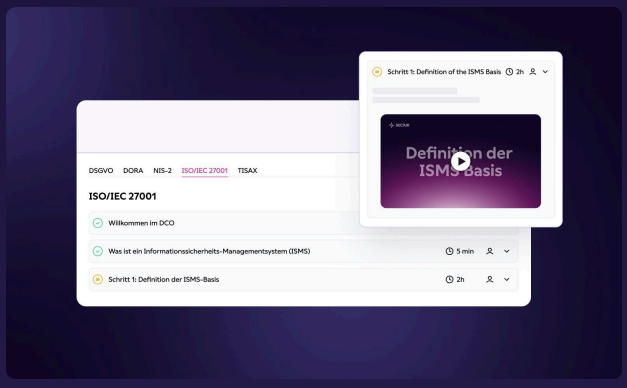
SECJUR

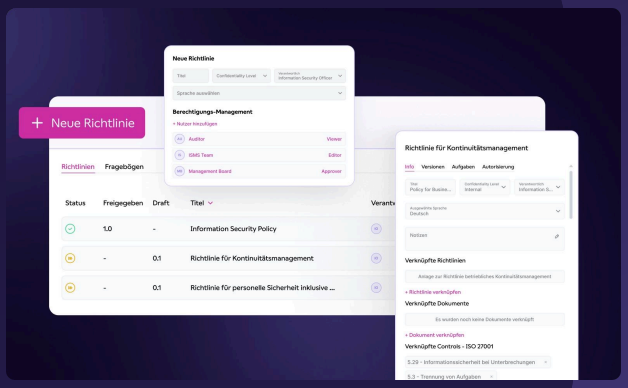
# Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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 ISO 27001:

## “Dank Kundenvertrauen auf die Financial-Times-1000-Liste”

**René Schlüß**
Founder & Managing Director, reanmo

reanmo

**FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR**

Masterplan.com · 1KOMMA5° · yfood · deepset · Tomorrow · AllDent Zahnzentrum

www.secjur.com