SECJUR

ISO/IEC 27001 Checkliste für Startups

Was Founder & CEOs wissen müssen — von der ersten Policy bis zum Zertifizierungsaudit.

Informationssicherheit läuft in Startups lange im Schatten von Produkt und Wachstum. Der Anstoß kommt häufig von außen: ein **Enterprise-Kunde** fordert im Onboarding einen Nachweis, ein **Investor** prüft in der Due Diligence systematisch Datenschutz und Sicherheitsprozesse, oder ein strategischer Käufer macht das **ISMS zur Voraussetzung** für den Deal. **ISO/IEC 27001** ist der Standard, an dem sich all diese Gespräche ausrichten — ein Werkzeug, um Vertrauen **messbar und überprüfbar** zu machen.

Wann ISO 27001 für Startups entscheidend wird:

TREIBER 01

Kundenanforderung & Vertrieb

Enterprise-Kunden und öffentliche Auftraggeber verlangen standardisierte Vendor Assessments. Ohne ISMS fallen Startups in der **Vorqualifizierung** heraus — bevor das Pitch-Gespräch beginnt.

TREIBER 02

Enterprise-Zusammenarbeit

Auch nach Vertragsabschluss bleibt Sicherheit Dauerthema: **Sicherheitsfragebögen**, Audit-Rechte, DPA-Anhänge. Ein Zertifikat ersetzt Einzelnachweise und **beschleunigt das Onboarding.**

TREIBER 03

Fundraising & Due Diligence

In der **Tech-Due-Diligence** prüfen Investoren systematisch Datenverarbeitung und Incident Response. Ein laufendes ISMS reduziert **rote Flaggen** bei Bewertung und Term Sheet.

TREIBER 04

M&A & Exit

Strategische Käufer bewerten Sicherheit als **Risiko- und Haftungsfrage.** Lücken führen zu Kaufpreisabschlägen oder Earn-out-Klauseln — eine Zertifizierung **schützt die Bewertung.**

3–6 Monate

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

93 Controls

automatisiert nachweisbar — von **Asset-Register** bis **Incident Response**

1 Zertifikat

ersetzt unzählige **Vendor-Fragebögen** und beschleunigt Enterprise-Onboardings

SECJUR

Euer Weg zum ISMS — Schritt 1 bis 6

Die ersten sechs Schritte schaffen das Fundament: Scope, Management-Commitment, Asset-Transparenz und eine belastbare Risikobasis.

SCHRITT 01

Scope & Kontext

- [ ] **Anwendungsbereich** des ISMS schriftlich definieren (Systeme, Team, Produkt)
- [ ] **Stakeholder** und ihre Sicherheitsanforderungen identifizieren
- [ ] Interne und externe **Einflussfaktoren** dokumentieren
- [ ] **Scope-Dokument** vom Management freigeben lassen
- [ ] **Ausschlüsse** begründen und schriftlich festhalten
- [ ] **Review-Zyklus** für den Scope alle 12 Monate einplanen

SCHRITT 02

Management-Commitment

- [ ] **Informationssicherheitsleitlinie** vom Management verabschieden
- [ ] **Budget und Ressourcen** formal zuweisen und dokumentieren
- [ ] **Verantwortliche:n** für Informationssicherheit benennen
- [ ] Sichtbares **Commitment der Geschäftsführung** sichern
- [ ] Rolle in der **Aufbauorganisation** verankern
- [ ] Fortschritt **quartalsweise an Board** oder Investoren reporten

SCHRITT 03

Asset-Register aufbauen

- [ ] **IT-Systeme,** Endgeräte und Cloud-Services vollständig erfassen
- [ ] **SaaS-Tools** und externe Datenverarbeitungen aufnehmen
- [ ] **Kundendaten** und kritische IP klassifizieren
- [ ] **Eigentümer** je Asset zuweisen
- [ ] **Schutzbedarf** je Asset einstufen (CIA-Triade)
- [ ] **ISMS-Plattform** oder Tooling für Asset-Management einsetzen

SCHRITT 04

Risiken bewerten

- [ ] **Bedrohungen** und Schwachstellen je Asset identifizieren
- [ ] **Datenpannen-** und Reputationsszenarien systematisch bewerten
- [ ] **Eintrittswahrscheinlichkeit** und Schadenshöhe einschätzen
- [ ] Risiken **priorisieren** und im Register dokumentieren
- [ ] **Risikoakzeptanzkriterien** mit der GF formell abstimmen
- [ ] **Risikoregister** in ISMS-Plattform führen und aktuell halten

SCHRITT 05

Maßnahmen & SoA

- [ ] **Controls** aus ISO 27001 Anhang A auswählen
- [ ] **Statement of Applicability** erstellen und begründen
- [ ] **Maßnahmenplan** mit Terminen und Verantwortlichen aufsetzen
- [ ] **Budget** je Maßnahme zuordnen und freigeben lassen
- [ ] **Begründung** für jeden ausgeschlossenen Control festhalten
- [ ] **SoA** bei Scope-Änderungen regelmäßig aktualisieren

SCHRITT 06

Leitlinien & Richtlinien

- [ ] **Informationssicherheitsleitlinie** verabschieden und kommunizieren
- [ ] **Zugriffs- und Passwortrichtlinien** verbindlich festlegen
- [ ] **Remote-Arbeit** und Cloud-Nutzung klar regeln
- [ ] **Dokumentenlenkung** mit Versionierung und Freigabeprozess etablieren
- [ ] **Vendor-Richtlinien** und NDA-Prozesse für Dritte ergänzen
- [ ] Alle Richtlinien **jährlich reviewen** und bei Bedarf anpassen

SECJUR

Euer Weg zum ISMS — Schritt 7 bis 12

Die zweite Hälfte bringt das ISMS in den Betrieb: technische Maßnahmen, Lieferkette, Awareness, Audit und Zertifizierung.

SCHRITT 07

Technische Controls

- [ ] **Multi-Faktor-Authentifizierung** für alle kritischen Systeme aktivieren
- [ ] **Patch- und Schwachstellenmanagement** strukturiert aufsetzen
- [ ] **Backups und Wiederherstellung** regelmäßig testen
- [ ] **Zugriffsrechte** nach Need-to-know-Prinzip vergeben
- [ ] **Monitoring und Logging** zentral einrichten
- [ ] **Verschlüsselung** für Daten in Transit und at Rest aktivieren

SCHRITT 08

Lieferkette absichern

- [ ] **Kritische Dienstleister** und SaaS-Anbieter systematisch bewerten
- [ ] **Sicherheitsanforderungen** vertraglich verankern (AVV/DPA)
- [ ] **Cloud-Zugriffe** und API-Verbindungen kontrollieren und dokumentieren
- [ ] **Datenaustausch** mit Partnern und Kunden absichern
- [ ] **Lieferanten** mindestens jährlich nachprüfen
- [ ] **Sub-Processor-Liste** für DSGVO-Konformität aktuell halten

SCHRITT 09

Awareness & Notfall

- [ ] **Mitarbeitende** verpflichtend schulen (Security Awareness)
- [ ] **Incident-Response-Prozess** klar definieren und dokumentieren
- [ ] **Meldewege** nach DSGVO Art. 33 und intern festlegen
- [ ] **Phishing-Tests** und Auffrischungsschulungen einplanen
- [ ] **Notfallübung** mindestens einmal jährlich durchführen
- [ ] **Security-Champion** im Team benennen und einbinden

SCHRITT 10

Internes Audit & Review

- [ ] **Internes Audit** für das gesamte ISMS planen und durchführen
- [ ] **Abweichungen** (Nonconformities) und Korrekturmaßnahmen erfassen
- [ ] **Managementbewertung** mit der GF mindestens jährlich abhalten
- [ ] **Wirksamkeit der Controls** anhand von KPIs prüfen
- [ ] **Korrekturmaßnahmen** fristgerecht nachverfolgen
- [ ] **Audit-Ergebnisse** direkt in den nächsten PDCA-Zyklus einfließen lassen

SCHRITT 11

Zertifizierungsaudit

- [ ] **Akkreditierte Zertifizierungsstelle** (DAkkS) frühzeitig wählen
- [ ] **Stage-1-Audit** (Dokumentenprüfung) vollständig vorbereiten
- [ ] **Stage-2-Audit** (Vor-Ort-Prüfung) aktiv begleiten
- [ ] **Zertifikat** erhalten, kommunizieren und im Vertrieb einsetzen
- [ ] **Audit-Findings** fristgerecht und systematisch abarbeiten
- [ ] **Re-Zertifizierungsplan** nach 3 Jahren rechtzeitig aufsetzen

SCHRITT 12

ISMS am Leben halten

- [ ] **Kontinuierliche Verbesserung (KVP)** fest im ISMS verankern
- [ ] **Überwachungsaudits** jährlich einplanen und vorbereiten
- [ ] Neue **Produkte, Features und Systeme** direkt ins ISMS aufnehmen
- [ ] Mit **Plattform statt Excel** effizient pflegen und nachweisen
- [ ] **Kennzahlen** quartalsweise an GF und Board berichten
- [ ] **ISMS-Reifegrad** jährlich extern benchmarken lassen

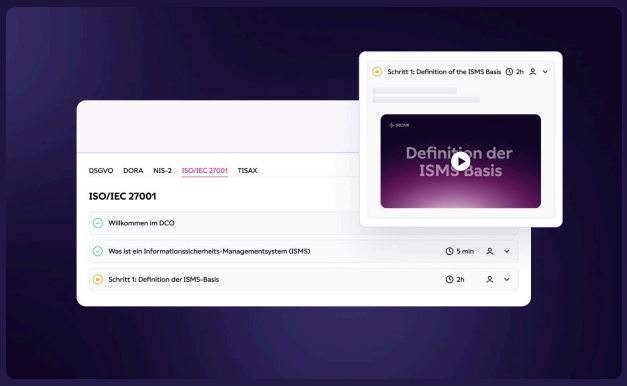
SECJUR

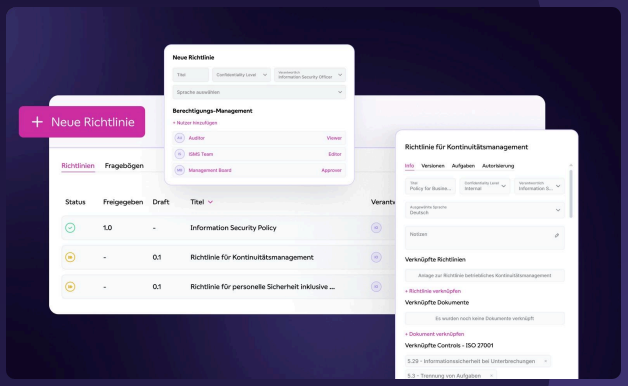
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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° · Tomorrow · deepset · yfood · vestlane

www.secjur.com