SECJUR

ISO/IEC 27001 für Software- & IT-Unternehmen

Der praktische Fahrplan zum ISMS für Gründer und CEOs in der Software- und IT-Branche: von der ersten Kundenanforderung bis zum Zertifikat.

Für Software- und IT-Unternehmen ist Informationssicherheit kein reines Compliance-Thema. Der Anstoß kommt meist von außen: ein Enterprise-Kunde stellt konkrete Security-Anforderungen im Vendor Assessment, Investoren prüfen in der Due Diligence systematisch die IT-Sicherheit, oder **NIS-2** schafft erstmals gesetzliche Pflichten für IT-Dienstleister. Gründer und CEOs spüren diesen Druck zuerst und müssen das Thema strukturiert angehen. **ISO/IEC 27001** ist der Standard, an dem sich all diese Anforderungen ausrichten: ein Werkzeug, um Cloud-Infrastruktur, Kundendaten und Quellcode **nachweisbar abzusichern** und Vertrauen gegenüber Kunden, Investoren und Regulatoren messbar zu machen.

Wann ISO 27001 für Software- und IT-Unternehmen konkret wird:

TREIBER 01

Enterprise-Aufträge in der Lieferkette

Größere B2B-Kunden und öffentliche Auftraggeber verlangen im Onboarding standardisierte Vendor Assessments und Sicherheitsnachweise. Ohne ISMS oder belastbare Roadmap scheiden Software-Anbieter in der Vorqualifizierung aus und verlieren Aufträge an zertifizierte Wettbewerber.

TREIBER 02

Investoren-Due-Diligence & Fundraising

VCs und strategische Investoren prüfen in der Tech-Due-Diligence systematisch Datenschutz, Zugriffskontrolle und Incident Response. Ein laufendes ISMS oder vorhandenes Zertifikat reduziert rote Flaggen und sichert **Bewertung und Term Sheet.**

TREIBER 03

NIS-2 & gesetzliche Pflicht

Mit dem NIS2UmsuCG fallen viele **IT-Dienstleister und Software-Anbieter** erstmals in einen verbindlichen Pflichtenkreis: Risikomanagement, Meldewege, Lieferkettensicherheit. ISO 27001 liefert das Rahmenwerk, um diese Anforderungen **strukturiert und prüffest** umzusetzen.

TREIBER 04

Schutz von Quellcode & Kundendaten

Quellcode, Architekturpläne und Kundendaten sind das Kapital von Software-Unternehmen und ein Ziel für Angreifer. Ein gelebtes ISMS schützt geistiges Eigentum über **Zugriffskontrolle, Klassifizierung** und gesicherte Austauschwege mit Partnern und Sub-Contractoren.

3 bis 6 Monate

typische Umsetzungszeit mit Plattform & Expert:innen, statt 12+ Monate im Eigenbau neben dem Tagesgeschäft

Ein Zertifikat

ersetzt unzählige Vendor-Fragebögen und beschleunigt das Enterprise-Onboarding bei Kunden spürbar

93 Controls

nach ISO 27001:2022 Anhang A, alle automatisiert nachweisbar und auditfähig über eine Plattform

SECJUR

Ihr Weg zum ISMS: Schritt 1 bis 6

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

SCHRITT 01

Management-Auftrag gewinnen

- [ ] **Auslöser** dokumentieren (Kunde, Investor, NIS-2, Konzern)
- [ ] **Budget und Ressourcen** freigeben lassen
- [ ] **Verantwortliche:n** für Informationssicherheit benennen
- [ ] Sichtbares **Commitment der GF** einholen
- [ ] Rolle in der **Aufbauorganisation** verankern
- [ ] **Projektplan** und Timeline für die Implementierung erstellen

SCHRITT 02

Geltungsbereich definieren

- [ ] **Produkte und Services** in den Scope aufnehmen
- [ ] **Cloud-Infrastruktur** und SaaS-Tools abgrenzen
- [ ] **Externe Entwickler** und Sub-Contractor einbeziehen
- [ ] **Scope** schriftlich fixieren und freigeben
- [ ] **Ausschlüsse** begründen und dokumentieren
- [ ] **Scope-Dokument** intern kommunizieren und abstimmen

SCHRITT 03

Asset-Register aufbauen

- [ ] **IT-Systeme**, Cloud-Ressourcen und Endgeräte erfassen
- [ ] **Quellcode-Repositories** und Entwicklungsumgebungen aufnehmen
- [ ] **Kundendaten** und SaaS-Zugänge klassifizieren
- [ ] **Verantwortlichkeiten** je Asset zuweisen
- [ ] **Schutzbedarf** je Asset einstufen
- [ ] **Lebenszyklusstatus** und Eigentümer je Asset pflegen

SCHRITT 04

Risiken bewerten

- [ ] **Bedrohungen** für Cloud, Code und Kundensysteme identifizieren
- [ ] **Datenpannen-** und **Zugriffsrisiken** bewerten
- [ ] **Eintritt und Schadenshöhe** einschätzen
- [ ] **Risiken** priorisieren und dokumentieren
- [ ] **Risikoakzeptanzkriterien** mit der GF abstimmen
- [ ] **Risikobehandlungsplan** erstellen und freigeben lassen

SCHRITT 05

Maßnahmen festlegen (SoA)

- [ ] **Controls** aus Anhang A der ISO 27001:2022 auswählen
- [ ] **Statement of Applicability** erstellen
- [ ] **Maßnahmenplan** mit Terminen aufsetzen
- [ ] **Verantwortliche und Budget** zuordnen
- [ ] **Begründung** je Control festhalten
- [ ] **Fortschritt** je Control regelmäßig nachverfolgen

SCHRITT 06

Richtlinien erstellen

- [ ] **Informationssicherheitsleitlinie** verabschieden
- [ ] **Zugriffs- und Passwortrichtlinien** festlegen
- [ ] Regeln für **Remotezugriff** und **BYOD** definieren
- [ ] **Secure-SDLC**-Anforderungen dokumentieren
- [ ] **Lieferanten-** und Sub-Contractor-Richtlinien ergänzen
- [ ] **Richtlinien** allen Mitarbeitenden kommunizieren und schulen

SECJUR

Ihr Weg zum ISMS: Schritt 7 bis 12

Die zweite Hälfte bringt das ISMS in den Betrieb: technische Härtung, Lieferkettensicherheit, Notfallvorsorge, internes Audit, Zertifizierung und den laufenden Betrieb.

SCHRITT 07

Technische Controls umsetzen

- [ ] **MFA** für alle Konten und kritischen Zugänge einführen
- [ ] **Patch- und Schwachstellenmanagement** aufsetzen
- [ ] **Backups** und Wiederherstellung regelmäßig testen
- [ ] **Zugriffsrechte** nach Need-to-know vergeben
- [ ] **Monitoring und Logging** einrichten
- [ ] **Penetrationstests** für kritische Systeme einplanen

SCHRITT 08

Lieferkette absichern

- [ ] **Kritische Dienstleister** und SaaS-Anbieter bewerten
- [ ] **Sicherheitsanforderungen** vertraglich verankern
- [ ] **Zugänge** externer Entwickler kontrollieren
- [ ] **Datenaustausch** mit Kunden und Partnern absichern
- [ ] **Sub-Contractor** regelmäßig nachprüfen
- [ ] **Notfallkontakte** bei Dienstleistern hinterlegen

SCHRITT 09

Awareness & Incident Response

- [ ] **Mitarbeitende** regelmäßig zu IT-Sicherheit schulen
- [ ] **Incident-Response-Prozess** definieren
- [ ] **Meldewege** (auch DSGVO / NIS-2) festlegen
- [ ] **Notfallübungen** für Sicherheitsvorfälle durchführen
- [ ] **Phishing-Tests** und Auffrischungen einplanen
- [ ] **Lessons Learned** aus Vorfällen dokumentieren

SCHRITT 10

Internes Audit & Review

- [ ] **Internes Audit** planen und durchführen
- [ ] **Abweichungen** und Korrekturmaßnahmen erfassen
- [ ] **Managementbewertung** mit der GF abhalten
- [ ] **Wirksamkeit** der Controls prüfen
- [ ] **Korrekturmaßnahmen** nachverfolgen
- [ ] **Audit-Ergebnisse** dokumentieren und archivieren

SCHRITT 11

Zertifizierungsaudit bestehen

- [ ] **Akkreditierte Zertifizierungsstelle** wählen
- [ ] **Stage-1-Audit** (Dokumentation) vorbereiten
- [ ] **Stage-2-Audit** (Umsetzung) begleiten
- [ ] **Zertifikat** erhalten und kommunizieren
- [ ] **Audit-Findings** systematisch abarbeiten
- [ ] **Zertifikat** in Angeboten und auf der Website einsetzen

SCHRITT 12

ISMS am Leben halten

- [ ] **Kontinuierliche Verbesserung** (KVP) verankern
- [ ] **Überwachungsaudits** jährlich einplanen
- [ ] Neue **Produkte und Services** direkt ins ISMS aufnehmen
- [ ] Mit **Plattform statt Excel** pflegen
- [ ] **Kennzahlen** regelmäßig an die GF berichten
- [ ] **Zertifizierungsumfang** bei Änderungen anpassen

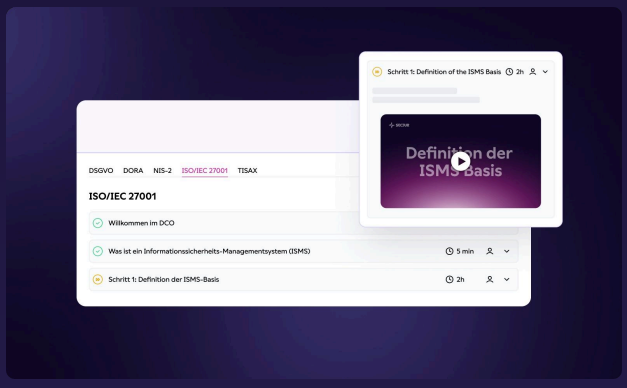
SECJUR

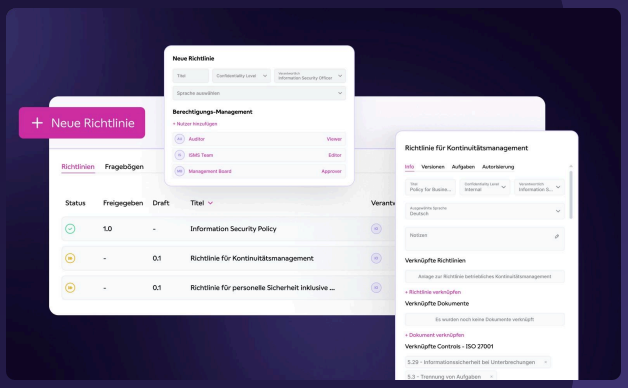
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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

deepset · Masterplan.com · team internet. · think-cell · statista · WatchGuard

www.secjur.com