SECJUR

ISO/IEC 27001 für IT-Systemhäuser

Der praktische Fahrplan zur Zertifizierung für Founder & Geschäftsführer — von der ersten Kundenanforderung bis zum Zertifikat.

IT-Systemhäuser stehen unter doppeltem Druck: Als Dienstleister tragen sie Verantwortung für die Informationssicherheit ihrer Kunden — und geraten gleichzeitig als kritische Zulieferer selbst in den Fokus regulatorischer Anforderungen. **ISO/IEC 27001** ist dabei nicht nur ein Zertifikat, sondern der strukturierte Rahmen, um Sicherheit nachweisbar zu machen — gegenüber Enterprise-Kunden, Auditoren und dem eigenen Management.

Wann ISO 27001 für IT-Systemhäuser konkret wird:

TREIBER 01

Kundenforderungen & Ausschreibungen

Enterprise-Kunden und öffentliche Auftraggeber verlangen ISO 27001-Zertifikate als Mindestanforderung. Ohne Nachweis scheitern IT-Systemhäuser in der Vorqualifizierung — bevor das erste Gespräch stattfindet.

TREIBER 02

NIS2 & gesetzliche Pflichten

Mit dem **NIS2UmsuCG** rücken IT-Systemhäuser als kritische Dienstleister in einen verbindlichen Pflichtenkreis: Risikomanagement, Meldewege, Lieferkettensicherheit. ISO 27001 liefert das Rahmenwerk zur prüffesten Umsetzung.

TREIBER 03

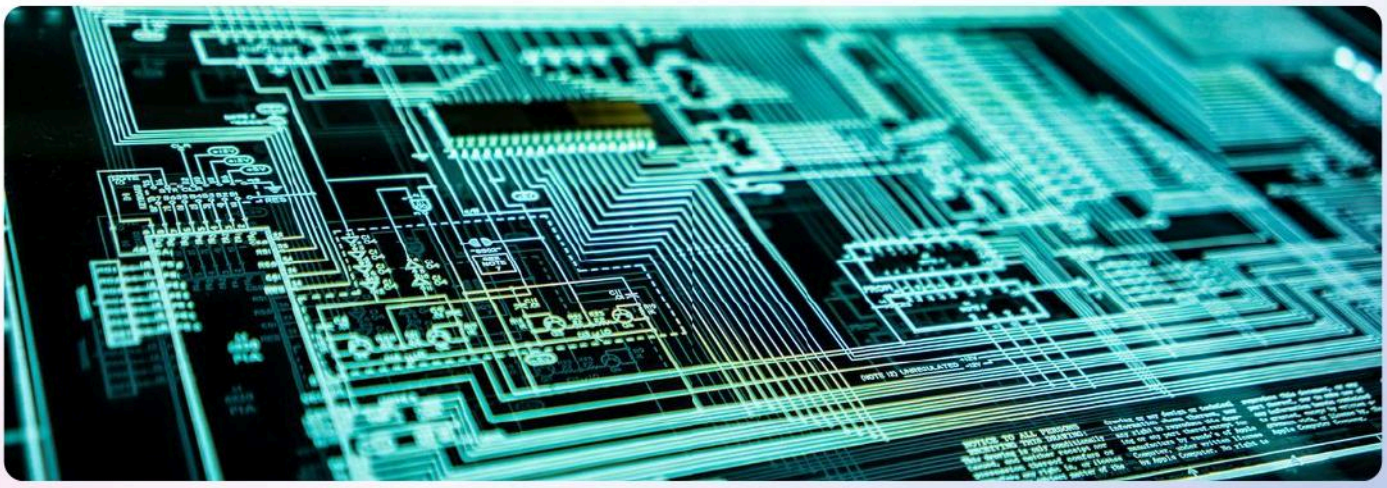
Wettbewerbsdifferenzierung

Im gesättigten IT-Systemhaus-Markt ist ISO 27001 ein **messbares Differenzierungsmerkmal.** Das Zertifikat signalisiert Prozessreife — und überzeugt in Vergabeprozessen ohne langes Erklären.

TREIBER 04

Haftung & Geschäftsführerpflicht

Bei Sicherheitsvorfällen haften Geschäftsführer **persönlich.** Ein funktionierendes ISMS ist der nachweisbare Beleg für pflichtgemäßes Handeln — und schützt Kundendaten sowie Betriebsgeheimnisse.



3–6 Monate

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

Ein Zertifikat

ersetzt **unzählige Kunden-Fragebögen** und beschleunigt Enterprise-Onboarding spürbar

93 Controls

der ISO 27001:2022 — von **Asset-Register** bis Lieferantenmanagement systematisch abgedeckt

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 das IT-Systemhaus.

SCHRITT 01

Auftrag & Geschäftsführung gewinnen

- [ ] **Auslöser** dokumentieren (Kunde, NIS2-Prüfung, Konzernvorgabe)
- [ ] **Budget und Ressourcen** freigeben lassen
- [ ] **Verantwortliche:n** für Informationssicherheit benennen
- [ ] **Commitment der GF** sichtbar einholen und dokumentieren
- [ ] **ISB-Funktion** intern besetzen oder extern vergeben

SCHRITT 02

Geltungsbereich definieren

- [ ] **Standorte und Betriebsbereiche** abgrenzen
- [ ] **IT-Services, Cloud-Dienste** und Kundenportale einbeziehen
- [ ] **Kritische Kundenschnittstellen** erfassen
- [ ] **Scope** sauber dokumentieren
- [ ] **Ausschlüsse** begründen und festhalten

SCHRITT 03

Asset-Register aufbauen

- [ ] **Server, Clients** und Cloud-Ressourcen erfassen
- [ ] **Managed-Services-Systeme** und Kundenzugänge aufnehmen
- [ ] **Kundendaten** und Konfigurationen klassifizieren
- [ ] **Verantwortlichkeiten** je Asset zuweisen
- [ ] **Schutzbedarf** je Asset einstufen

SCHRITT 04

Risiken bewerten

- [ ] **Bedrohungen** für Kundenprojekte und Infrastruktur identifizieren
- [ ] **Ransomware-** und Datenverlust-Szenarien bewerten
- [ ] **Eintritt und Schadenshöhe** einschätzen
- [ ] **Risiken** priorisieren und dokumentieren
- [ ] **Risikoakzeptanzkriterien** mit der GF abstimmen

SCHRITT 05

Maßnahmen festlegen (SoA)

- [ ] **Controls** aus Annex A auswählen
- [ ] **Statement of Applicability** erstellen
- [ ] **Maßnahmenplan** mit Terminen aufsetzen
- [ ] **Verantwortliche** und Budget zuordnen
- [ ] **Begründung** je Control festhalten

SCHRITT 06

Leitlinien & Richtlinien erstellen

- [ ] **Informationssicherheitsleitlinie** verabschieden
- [ ] **Zugriffs- und Passwortrichtlinien** festlegen
- [ ] **Remote-Zugriff** und BYOD regeln
- [ ] **Dokumentenlenkung** etablieren
- [ ] **Kunden- und Lieferantenrichtlinien** ergänzen

SECJUR

Ihr Weg zum ISMS — Schritt 7 bis 12

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

SCHRITT 07

Technische Maßnahmen umsetzen

- [ ] **Netzwerke segmentieren** (interne und Kundennetzwerke trennen)
- [ ] **Patch- und Schwachstellenmanagement** aufsetzen
- [ ] **Backups und Wiederherstellung** regelmäßig testen
- [ ] **Zugriffsrechte** nach Need-to-know vergeben
- [ ] **Monitoring und Logging** einrichten

SCHRITT 08

Lieferkette & Kundenprojekte absichern

- [ ] **Kritische Dienstleister** und Subunternehmer bewerten
- [ ] **Sicherheitsanforderungen** vertraglich verankern
- [ ] **Remote-Wartungszugänge** zu Kunden kontrollieren
- [ ] **Datenaustausch** verschlüsselt absichern
- [ ] **Lieferanten** regelmäßig nachprüfen

SCHRITT 09

Awareness & Notfallvorsorge

- [ ] **Mitarbeitende** regelmäßig schulen
- [ ] **Incident-Response-Prozess** definieren
- [ ] **Meldewege** (auch NIS2/DSGVO) festlegen
- [ ] **Notfallübungen** und Wiederherstellungstests durchführen
- [ ] **Phishing-Tests** und Auffrischungen einplanen

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

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

SCHRITT 12

ISMS am Leben halten

- [ ] **Kontinuierliche Verbesserung** (KVP) verankern
- [ ] **Überwachungsaudits** jährlich einplanen
- [ ] **Neue Projekte** direkt ins ISMS aufnehmen
- [ ] **Mit Plattform** statt Excel pflegen
- [ ] **Kennzahlen** regelmäßig an die GF berichten

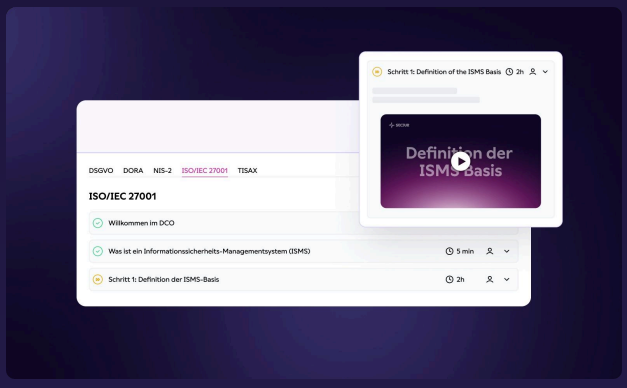
SECJUR

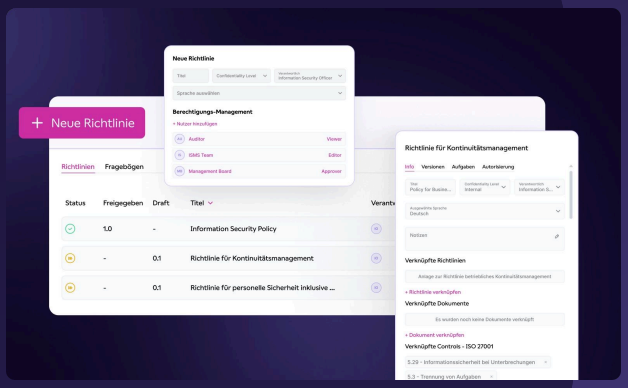
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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

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

www.secjur.com