SECJUR

ISO/IEC 27001 für Industrie & Maschinenbau

Der praktische Fahrplan zum ISMS für IT-Leiter:innen im produzierenden Mittelstand — von der Kundenanforderung bis zum Zertifikat.

Im Maschinenbau und der Fertigung wird Informationssicherheit selten aus eigenem Antrieb zum Projekt. Der Anstoß kommt von außen: ein Großkunde fordert im Lieferantenfragebogen den Nachweis, die Konzernmutter zieht Vorgaben hoch, oder **NIS2** bringt erstmals gesetzliche Pflichten ins Spiel. Die IT-Leitung spürt diesen Druck zuerst — und trägt das Thema dann in die Geschäftsführung. **ISO/IEC 27001** ist der Standard, an dem sich all diese Anforderungen ausrichten: ein Werkzeug, um vernetzte Produktion, OT-Systeme und sensibles Konstruktions-Know-how **nachweisbar abzusichern** — statt jeden Kunden einzeln zu überzeugen.

Wann ISO 27001 im Maschinenbau konkret wird:

TREIBER 01

Kundenanforderung in der Lieferkette

OEMs und Großkunden verlangen im Onboarding standardisierte Lieferantenfragebögen und Sicherheitsnachweise. Ohne ISMS oder belastbare Roadmap fallen Zulieferer in der Vorqualifizierung heraus — und **verlieren Aufträge** an zertifizierte Wettbewerber.

TREIBER 02

NIS2 & gesetzliche Pflicht

Mit dem **NIS2UmsuCG** fallen viele Industrieunternehmen erstmals in einen **verbindlichen Pflichtenkreis:** Risikomanagement, Meldewege, Lieferkettensicherheit. ISO 27001 liefert das Rahmenwerk, mit dem sich diese Anforderungen **strukturiert und prüffest** umsetzen lassen.

TREIBER 03

Vernetzte Produktion & OT

Smart Factory, vernetzte Maschinen und IT/OT-Konvergenz vergrößern die **Angriffsfläche** erheblich. Ein Produktionsstillstand durch **Ransomware** kostet sofort sechsstellig. Das ISMS bringt **Asset-Transparenz, Segmentierung** und Notfallprozesse in genau diese Umgebung.

TREIBER 04

Schutz des Konstruktions-Know-hows

Konstruktionsdaten, CAD-Modelle und Fertigungsverfahren sind das Kapital im Maschinenbau und ein Ziel für **Industriespionage.** Ein gelebtes ISMS schützt geistiges Eigentum über **Zugriffskontrolle, Klassifizierung** und gesicherte Austauschwege mit Partnern.

3–6 Monate

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

Ein Nachweis

ersetzt **unzählige Kunden-Fragebögen** und beschleunigt das Lieferanten-Onboarding bei OEMs spürbar

IT & OT

Office-IT und Produktionsumgebung in **einem gemeinsamen Sicherheitsrahmen** statt isolierter Insellösungen

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 vernetzte Produktion.

SCHRITT 01

Auftrag & Geschäftsführung gewinnen

- [ ] **Auslöser** dokumentieren (Kunde, NIS2, Konzern)
- [ ] **Budget und Ressourcen** freigeben lassen
- [ ] **Verantwortliche:n** für Informationssicherheit benennen
- [ ] Sichtbares **Commitment der GF** einholen
- [ ] Rolle in der **Aufbauorganisation** verankern

SCHRITT 02

Geltungsbereich definieren

- [ ] **Standorte und Werke** abgrenzen
- [ ] **Office-IT und OT/Produktion** einbeziehen
- [ ] **Kritische Prozesse** und Schnittstellen erfassen
- [ ] **Scope** sauber dokumentieren
- [ ] **Ausschlüsse** begründen und festhalten

SCHRITT 03

Asset-Register aufbauen

- [ ] **IT-Systeme** , Server und Endgeräte erfassen
- [ ] **Maschinen, SPS** und vernetzte Anlagen aufnehmen
- [ ] **Konstruktions- und CAD-Daten** klassifizieren
- [ ] **Verantwortlichkeiten** je Asset zuweisen
- [ ] **Schutzbedarf** je Asset einstufen

SCHRITT 04

Risiken bewerten

- [ ] **Bedrohungen für IT und OT** identifizieren
- [ ] **Ransomware- und Stillstand-Szenarien** bewerten
- [ ] **Eintritt und Schadenshöhe** einschätzen
- [ ] Risiken **priorisieren** und dokumentieren
- [ ] **Risikoakzeptanzkriterien** mit der GF abstimmen

SCHRITT 05

Maßnahmen festlegen (SoA)

- [ ] **Controls aus Anhang 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
- [ ] Regeln für **Wechselmedien und Fernzugriff**
- [ ] **Dokumentenlenkung** etablieren
- [ ] **Lieferanten- und OT-Richtlinien** ergänzen

SECJUR

Ihr Weg zum ISMS — Schritt 7 bis 12

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

SCHRITT 07

Technische Maßnahmen umsetzen

- [ ] **Netze segmentieren** (IT/OT-Trennung)
- [ ] **Patch- und Schwachstellenmanagement** aufsetzen
- [ ] **Backups und Wiederherstellung** testen
- [ ] **Zugriffsrechte** nach Need-to-know vergeben
- [ ] **Monitoring und Logging** einrichten

SCHRITT 08

Lieferkette absichern

- [ ] **Kritische Dienstleister** und Partner bewerten
- [ ] **Sicherheitsanforderungen** vertraglich verankern
- [ ] **Fernwartungszugänge** kontrollieren
- [ ] **Datenaustausch mit OEMs** absichern
- [ ] Lieferanten **regelmäßig nachprüfen**

SCHRITT 09

Awareness & Notfallvorsorge

- [ ] **Mitarbeitende** regelmäßig schulen
- [ ] **Incident-Response-Prozess** definieren
- [ ] **Meldewege** (auch NIS2) festlegen
- [ ] **Notfallübung** in der Produktion 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

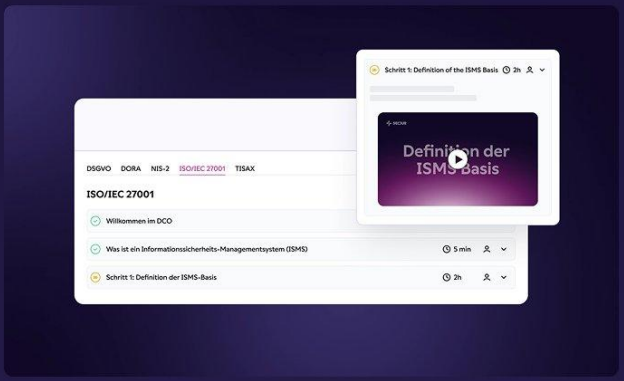
- [ ] **Kontinuierliche Verbesserung (KVP)** verankern
- [ ] **Überwachungsaudits** jährlich einplanen
- [ ] **Neue Maschinen** direkt ins ISMS aufnehmen
- [ ] Mit **Plattform statt Excel** pflegen
- [ ] **Kennzahlen** regelmäßig an die GF berichten

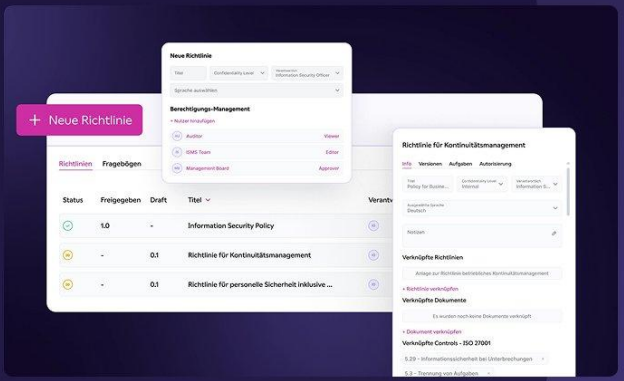
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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 zu Informationssicherheitszertifizierungen:

> “Wir konnten wie geplant neue OEM-Projekte erlangen und so den Unternehmensumsatz steigern. Die Plattform ist super hilfreich und unsere Ansprechpartnerin unterstützt uns stets kompetent.”

Steffen Brureiner
Projektleiter IT

KLEINER STANZTECHNIK
CoCREATE THE FUTURE

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR

SWT STAHLWERK THÜRINGEN · OTTO DÖRNER · oetinger aluminium · FEDDERSEN GRUPPE · STEYRMOTORS

www.secjur.com