SECJUR

ISO/IEC 27001 für Luftfahrt & Verteidigung

Was Founder und CEOs in regulierten Lieferketten wissen müssen — bevor der nächste Audit, die nächste Ausschreibung oder der nächste Deal kommt.

In der Luft- und Raumfahrt sowie der Verteidigungsindustrie entscheidet Informationssicherheit darüber, ob Unternehmen überhaupt zur Wahl stehen. Supply-Chain-Audits von OEMs, NADCAP-Anforderungen, NATO-Lieferbedingungen und behördliche Zulassungsverfahren verlangen belastbare Nachweise — nicht Versprechen. **ISO/IEC 27001** ist der international anerkannte Standard, der diese Nachweise liefert. Diese Checkliste gibt Ihnen als **Founder oder CEO eine strukturierte Übersicht**, worauf es in Ihrer Branche besonders ankommt.

Vier Felder, in denen ISO 27001 in Ihrer Branche direkt wirkt:

FELD 01

Lieferketten-Zulassung

OEMs wie Airbus, Boeing oder Rheinmetall prüfen ihre Zulieferer systematisch auf Informationssicherheit. Ohne Zertifikat oder glaubwürdige Roadmap droht der Ausschluss aus der qualifizierten Lieferantenliste — oft bevor das eigentliche Pitch-Gespräch beginnt.

FELD 02

Behördliche Zulassung & Export

ITAR, EAR, nationale Geheimschutzvorschriften und das BAFA erwarten dokumentierte Sicherheitskontrollen. ISO 27001 schafft die strukturelle Grundlage für diese Nachweisführung und reduziert Compliance-Aufwand deutlich.

FELD 03

Öffentliche Ausschreibungen

Vergabeverfahren der Bundeswehr, NATO und öffentlicher Rüstungsbeschaffung verlangen konkrete Sicherheitsnachweise. Ein ISO-27001-Zertifikat erhöht Bewerbungschancen messbar und reduziert den Aufwand in der Angebotsvorbereitung erheblich.

FELD 04

Investoren-Due-Diligence

Private-Equity- und strategische Investoren aus dem Aerospace- und Defense-Umfeld bewerten Informationssicherheit als zentrales Risikothema. Lücken führen zu Bewertungsabschlägen oder verhindern Transaktionen.

3–6 Monate

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

93 Controls

strukturiert nachweisbar — von Asset-Register bis Incident Response in einem Dashboard

1 Zertifikat

ersetzt unzählige Supply-Chain-Fragebögen und beschleunigt Zulassungsverfahren deutlich

SECJUR

Ihre ISO-27001-Checkliste

Sechs operative Schritte, die in der Luft- und Verteidigungsindustrie besonders kritisch sind.

SCHRITT 01

Anwendungsbereich & Scope

- [ ] ISMS-Scope auf sicherheitsrelevante Systeme, Pläne und Produktionsdaten eingrenzen
- [ ] Klassifikation nach Vertraulichkeitsstufe (bis VS-NfD) dokumentieren
- [ ] Schnittstellen zu OEM-Systemen und Behördenportalen im Scope erfassen
- [ ] Kritische Assets (CAD-Daten, Fertigungsparameter) inventarisieren
- [ ] Scope-Dokument formal freigeben und versionieren

SCHRITT 02

Risikoanalyse & Bedrohungen

- [ ] Branchenspezifische Bedrohungsakteure identifizieren (APTs, Industriespionage)
- [ ] Risikobewertung nach ISO 27005 oder NIST SP 800-30 durchführen
- [ ] Supply-Chain-Risiken durch Lieferanten systematisch erfassen
- [ ] Risikoakzeptanzkriterien mit Geschäftsführung abstimmen und dokumentieren
- [ ] Risikobehandlungsplan erstellen und Maßnahmen terminieren

SCHRITT 03

Zugriff & Least Privilege

- [ ] Rollenbasiertes Zugriffskonzept (RBAC) für alle kritischen Systeme einführen
- [ ] Privilegierte Accounts (Admin, CAD) mit MFA absichern
- [ ] Externe Zugriffe von OEMs über dedizierte Zugänge mit Protokollierung
- [ ] Quarterly Access Reviews für alle Benutzerkonten etablieren
- [ ] Zugriffsprotokolle automatisiert auswerten und aufbewahren

SCHRITT 04

Verschlüsselung & Datenschutz

- [ ] Technische Zeichnungen und Konstruktionsdaten verschlüsselt speichern
- [ ] E-Mail-Verschlüsselung für sensible Lieferantenkommunikation einführen
- [ ] ITAR/EAR-relevante Daten in geografisch abgegrenzten Systemen halten
- [ ] Schlüsselmanagement dokumentieren und regelmäßig rotieren
- [ ] Datenlöschung und Datenträgervernichtung nach BSI-Standard regeln

SCHRITT 05

Incident Response

- [ ] IR-Plan für branchenspezifische Szenarien erstellen (Datenleck an OEM, Produktionsstörung)
- [ ] Meldekette zu BSI, BAFA und ggf. NATO-Stellen definieren
- [ ] Eskalationsprotokoll für ITAR-Verstöße durch Cyberangriffe einrichten
- [ ] Mindestens jährliche Incident-Response-Übungen durchführen
- [ ] Post-Incident-Reviews dokumentieren und Lessons Learned einarbeiten

SCHRITT 06

Supply-Chain-Sicherheit

- [ ] Lieferantenbewertung nach Informationssicherheitskriterien einführen
- [ ] Sicherheitsanforderungen in alle relevanten Lieferantenverträge aufnehmen
- [ ] Kritische Sublieferanten zu eigenen Sicherheitsnachweisen verpflichten
- [ ] Supply-Chain-Risiken jährlich im Risikomanagement aktualisieren
- [ ] Audit-Rechte gegenüber kritischen Lieferanten vertraglich sichern

SECJUR

Ihre ISO-27001-Checkliste

Weitere Schritte bis zur Zertifizierung — mit spezifischen Anforderungen für Ihre Branche.

SCHRITT 07

Physische Sicherheit

- [ ] Sicherheitszonen für Fertigung, Entwicklung und Serverräume definieren
- [ ] Zutrittskontrolle mit Protokollierung für alle sicherheitsrelevanten Bereiche
- [ ] Regelung für externe Besucher (OEM-Auditoren, Behördenvertreter) dokumentieren
- [ ] Schutz vor Abhören in Besprechungsräumen prüfen (TSCM-Assessment)
- [ ] Kamera- und Alarmanlage für sicherheitsrelevante Bereiche prüfen

SCHRITT 08

Awareness & Schulung

- [ ] Pflichtschulung zu Informationssicherheit, ITAR/EAR-Grundlagen und Social Engineering
- [ ] Rollenspezifische Schulungen für Entwickler, Fertigung und Management
- [ ] Phishing-Simulationen mindestens zweimal jährlich durchführen
- [ ] Schulungsnachweis für Lieferanten und Subunternehmer einfordern

SCHRITT 09

Business Continuity

- [ ] BCP für kritische Fertigungs- und Entwicklungsprozesse erstellen
- [ ] RTO und RPO für alle produktionsrelevanten Systeme definieren
- [ ] Offline-Backup-Strategie für technische Dokumentation einführen
- [ ] BCP-Tests jährlich durchführen und mit OEM-Anforderungen abstimmen
- [ ] Notfallkommunikation mit Kunden und Behörden vorab abstimmen

SCHRITT 10

Audit & Management Review

- [ ] Audit-Plan mit branchenspezifischen Prüfschwerpunkten erstellen
- [ ] Management Review mit GF mindestens jährlich durchführen
- [ ] Abweichungen aus OEM-Audits in ISMS-Korrekturmaßahmensystem integrieren
- [ ] KPIs für Sicherheitslage (Vorfälle, offene Maßnahmen, Schulungsquoten) tracken
- [ ] Ergebnisse des Management Reviews nachweislich dokumentieren

SCHRITT 11

Zertifizierungsaudit vorbereiten

- [ ] Zertifizierungsstelle mit DAkkS-Akkreditierung und Branchenerfahrung wählen
- [ ] Stage-1-Audit terminieren und Unterlagen vollständig bereitstellen
- [ ] Statement of Applicability (SoA) finalisieren und mit Risikobehandlung abgleichen
- [ ] Zertifizierungstermin frühzeitig mit Kunden und Behörden kommunizieren
- [ ] Surveillance-Audit-Zyklus (jährlich) von Beginn an einplanen

SCHRITT 12

Nachzertifizierung & Surveillance

- [ ] Surveillance-Audit-Zyklus (jährlich) frühzeitig mit Zertifizierungsstelle planen
- [ ] Interne Audits und Management Reviews vor jedem Surveillance-Audit durchführen
- [ ] Änderungen im ISMS (neue Assets, Prozesse, Risiken) laufend dokumentieren
- [ ] Re-Zertifizierung nach 3 Jahren einplanen und Ressourcen rechtzeitig reservieren
- [ ] Zertifikatsstatus aktiv für Kunden- und Behördenkommunikation nutzen

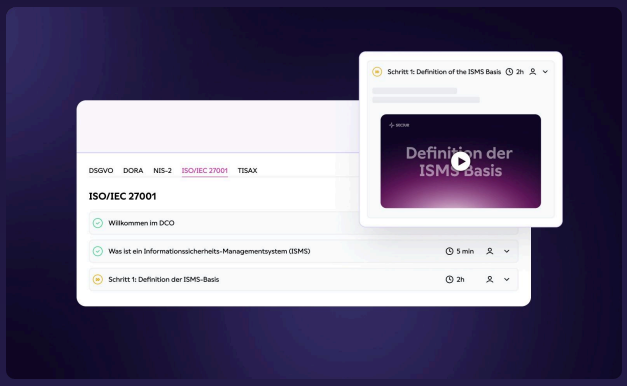
SECJUR

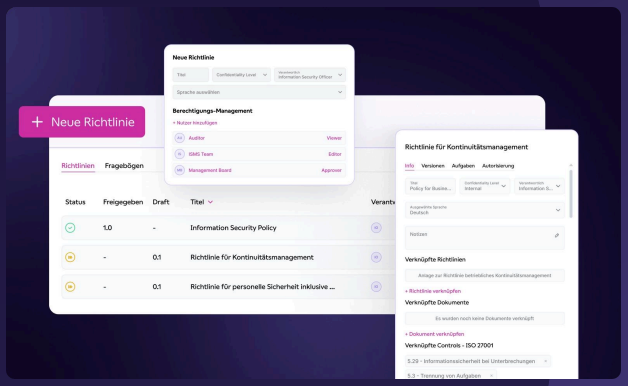
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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 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

STEYRMOTORS · CIRCUS GROUP · BECKHOFF New Automation Technology · Harmattan AI · TELESPAZIO a LEONARDO and THALES company · airsphere

www.secjur.com