SECJUR

ISO/IEC 27001 für Logistik

Was Founder und CEOs von Logistik-Unternehmen jetzt über Informationssicherheit wissen müssen – und warum die Zertifizierung zum Wettbewerbsvorteil wird.

Logistik-Unternehmen verarbeiten täglich sensible Daten: Lieferkettendaten, Kundenadressen, Zollinformationen, Telematikdaten ganzer Fahrzeugflotten. Gleichzeitig steigt der Druck von außen: Großkunden fordern Sicherheitsnachweise, die NIS2-Richtlinie erfasst zunehmend auch Logistikanbieter, und Ransomware-Angriffe häufen sich. **ISO/IEC 27001** ist der internationale Standard, der Informationssicherheit systematisch und auditierbar macht – und damit **aus einem Risiko einen messbaren Wettbewerbsvorteil**.

In diesen vier Bereichen entscheidet ISO 27001 in der Logistik:

SCHRITT 07

Kundenanforderungen

Automobilhersteller, Industrie- und Handelskonzerne setzen ISO 27001 bei Logistikdienstleistern als Mindestanforderung voraus. Ohne Zertifikat scheitern Ausschreibungen bereits in der Vorqualifizierung.

SCHRITT 08

Subunternehmer & Lieferkette

Spediteure und Subunternehmer sind ein zentrales Sicherheitsrisiko. ISO 27001 schreibt strukturiertes Lieferantenmanagement vor – und gibt Kunden den Nachweis, dass Standards entlang der Kette durchgesetzt werden.

SCHRITT 09

NIS2 & Regulierung

Die NIS2-Richtlinie stuft Logistik- und Transportdienstleister als wichtige Einrichtungen ein. Ein ISMS nach ISO 27001 deckt den Großteil der gesetzlichen Anforderungen ab.

SCHRITT 10

Cyberrisiken in der Logistik

Angriffe auf WMS, TMS und Telematikplattformen legen ganze Betriebe lahm. Ein ISO-27001-ISMS definiert verbindliche Controls für Netzwerksegmentierung, Backup und Incident Response.

3–6 Monate

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

93 Controls

automatisiert nachweisbar – von Asset-Register bis Incident Response auf einem Dashboard

Ein Zertifikat

ersetzt unzählige Sicherheitsfragebögen und beschleunigt Kunden-Onboardings deutlich

SECJUR

Die Checkliste: Schritte 1–6

Von der Vorbereitung bis zur Risikobewertung – Grundlagen eures Informationssicherheits-Managementsystems.

SCHRITT 01

ISMS-Scope definieren

- [ ] Relevante Systeme eingrenzen (WMS, TMS, Disposition, Fuhrpark)
- [ ] Kritische Assets im Logistikbetrieb identifizieren
- [ ] Scope-Dokument mit Geschäftsführung abstimmen
- [ ] Schnittstellen zu Kunden, Speditoren und Behörden festhalten

SCHRITT 02

Risikobewertung

- [ ] Bedrohungsszenarien dokumentieren (Ransomware, Datenverlust, Ausfall)
- [ ] Risiken für Telematik, Flottenmanagement und Kundendaten bewerten
- [ ] Subunternehmer-Risiken separat erfassen und gewichten
- [ ] Behandlungsoptionen pro Risiko festlegen und dokumentieren

SCHRITT 03

Richtlinien & Dokumentation

- [ ] Informationssicherheitsleitlinie durch Geschäftsführung verabschieden
- [ ] Asset-Register anlegen: Fahrzeuge, Systeme, Datenbestände
- [ ] Zugriffs- und Berechtigungskonzept erstellen
- [ ] Dokumentenlenkung und Versionierung einrichten

SCHRITT 04

Technische Controls

- [ ] Netzwerksegmentierung: Büro, Lager, Telematik und OBD trennen
- [ ] Patch-Management und Schwachstellen-Monitoring aufsetzen
- [ ] Datenverschlüsselung für Kunden- und Lieferscheindaten
- [ ] Backup- und Recovery-Prozesse testen und dokumentieren

SCHRITT 05

Mitarbeiterschulungen

- [ ] Schulungsplan für alle Rollen: Fahrer, Lager, Disposition, IT
- [ ] Pflichtschulung zu Phishing, Passwörtern und Gerätenutzung
- [ ] Awareness-Maßnahmen dokumentieren, Teilnahmen nachweisen
- [ ] Regelmäßige Auffrischung in den Jahreskalender integrieren

SCHRITT 06

Audit & Zertifizierung

- [ ] Internes Audit durch geschulte Person oder externe Unterstützung
- [ ] Management-Review durchführen und Ergebnisse dokumentieren
- [ ] Zertifizierungsstelle beauftragen (Stage-1- und Stage-2-Audit)
- [ ] Nonconformities schließen und Korrekturen nachweisen

SECJUR

Die Checkliste: Schritte 7–12

Von der Lieferkette bis zum Zertifizierungsaudit – logistikspezifische Anforderungen im ISMS.

SCHRITT 07

Lieferketten-Sicherheit

- [ ] Subunternehmer nach Sicherheitsanforderungen bewerten
- [ ] AVV und Sicherheitsklauseln in Verträge aufnehmen
- [ ] Regelmäßige Überprüfung von Dienstleisterzertifikaten
- [ ] Zugriffsrechte für externe Fahrer und Disponenten regeln

SCHRITT 08

Telematik & Fahrzeugdaten

- [ ] GPS- und Telematikdaten datenschutzkonform verarbeiten (DSGVO)
- [ ] OBD-Schnittstellen gegen unbefugte Zugriffe absichern
- [ ] Mobilgeräte der Fahrer per MDM verwalten, bei Verlust sperren
- [ ] Aufbewahrungsfristen für Tracking-Daten festlegen

SCHRITT 09

WMS & TMS absichern

- [ ] Rollenkonzept im Lagerverwaltungssystem (WMS) dokumentieren
- [ ] Zugriffsprotokollierung für kritische Systemfunktionen aktivieren
- [ ] Schnittstellen zu Kunden-ERP absichern (API-Keys, OAuth)
- [ ] Notfallbetrieb bei WMS-/TMS-Ausfall definieren und testen

SCHRITT 10

Kunden-EDI & Datenaustausch

- [ ] EDI-Verbindungen verschlüsseln, Zertifikate regelmäßig erneuern
- [ ] Zugriffsrechte auf Kundenportale rollenbasiert steuern
- [ ] Datenübertragungen protokollieren und auf Anomalien prüfen
- [ ] Kundenanforderungen aus Fragebögen zentral erfassen

SCHRITT 11

Incident Response

- [ ] Notfallplan für Ransomware, Systemausfall und Datenpanne erstellen
- [ ] Meldekette und Verantwortlichkeiten im Incident-Fall festlegen
- [ ] NIS2-Meldepflichten (72 Stunden) in den Prozess integrieren
- [ ] Jährliche Übungen und Tabletop-Tests durchführen

SCHRITT 12

Zertifizierungsaudit bestehen

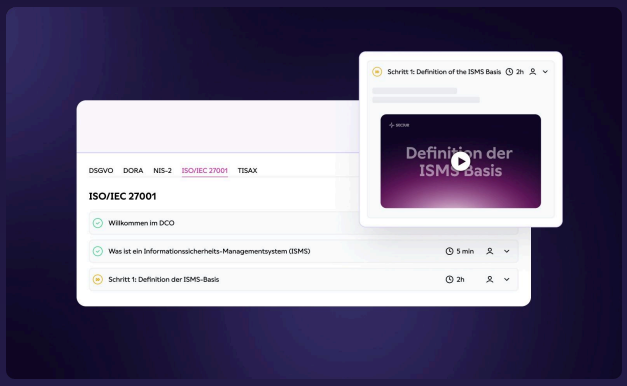
- [ ] Stage-1-Audit: Dokumentationsprüfung durch akkreditierte Stelle
- [ ] Stage-2-Audit: Nachweis der gelebten ISMS-Praxis vor Ort
- [ ] Nonconformities beheben und Korrekturen fristgerecht einreichen
- [ ] Zertifikat erhalten und intern sowie extern kommunizieren

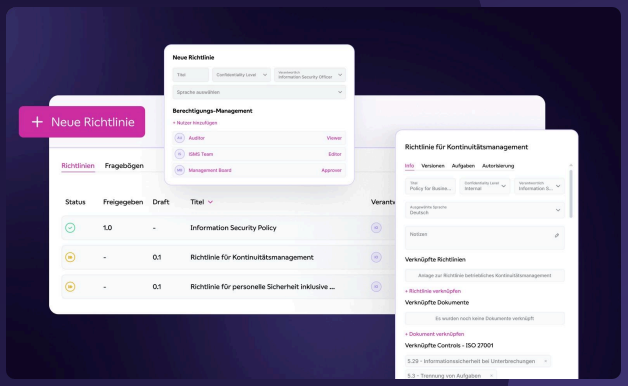
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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:

Dank SECJUR konnten wir schnell ein hochwertiges ISMS aufbauen, wie uns auch in den Zertifizierungsaudits bestätigt wurde. Unser zugewiesener Berater hat uns stets kompetent unterstützt - als wäre er ein Teil der Firma. Freuen uns auf die weitere Zusammenarbeit!

Stefan Gregori
Chief Information Security Officer

CONSOLINNO energy

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR

OTTO DÖRNER® SVG HEADWAY headwaylogistic gmbh bm bahndienste HADAG

www.secjur.com