SECJUR

ISO/IEC 27001 für die Lebensmittelbranche

Warum Informationssicherheit für Founder und CEOs in Food & Beverage heute kein Thema mehr ist, das warten kann.

Lieferketten werden digitaler, Produktionsdaten fließen in die Cloud, Handelspartner stellen systematische Sicherheitsanforderungen — und seit NIS2 gelten für viele Unternehmen der Lebensmittelbranche erstmals verbindliche Mindeststandards für Informationssicherheit. **ISO/IEC 27001** ist der internationale Rahmen, der all das zusammenführt: Er macht Sicherheit messbar, reduziert Haftungsrisiken und wird von Einkaufsabteilungen großer Handelskonzerne zunehmend als **Zugangsvoraussetzung** behandelt.

In vier Bereichen entscheidet ISO 27001 über Ihren Marktzugang:

BEREICH 01

Handelspartner & Listu...

Lebensmitteleinzelhändler und Großabnehmer verlangen von Lieferanten zunehmend Nachweise über Informationssicherheit — neben IFS Food und FSSC 22000. Ohne ISO 27001 oder belastbare Roadmap riskieren Sie Auslistung oder verzögerte Neulistung.

BEREICH 02

NIS2 & KRITIS-Pflicht...

Unternehmen der Lebensmittelbranche ab 250 Mitarbeitenden oder 50 Mio. EUR Umsatz können unter NIS2 als wichtige Einrichtung eingestuft werden. ISO 27001 ist der effizienteste Weg, §30-Anforderungen strukturiert nachzuweisen.

BEREICH 03

Digitale Lieferkette & ...

IoT-Sensoren, ERP-Anbindungen, digitale Traceability und vernetzte Produktionsanlagen vergrößern die Angriffsfläche massiv. Ein ISMS schützt IT- und OT-Umgebungen und adressiert Drittanbieterrisiken systematisch.

BEREICH 04

M&A, Investoren & E...

PE-Investoren und strategische Käufer prüfen im Due-Diligence-Prozess Datensicherheit und Compliance-Reifegrad. Lücken im ISMS führen zu Kaufpreisabschlägen — ein Zertifikat schützt die Unternehmensbewertung.

3–6 Monate

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

93 Controls

des ISO 27001:2022 Annex A — alle strukturiert dokumentiert und nachweisbar

1 Zertifikat

deckt Handelspartner-Fragebögen, NIS2-Nachweise und Investoren-Due-Diligence ab

SECJUR

Ihre ISO 27001 Checkliste

Von der Entscheidung bis zur Zertifizierung — die wichtigsten Schritte für Founder und CEOs in der Lebensmittelbranche.

SCHRITT 01

Scope & Geltungsbereich

- [ ] Welche Standorte, Systeme und Prozesse sollen zertifiziert werden?
- [ ] OT-Umgebungen und Produktionssteuerung explizit einschließen oder abgrenzen
- [ ] Schnittstellen zu Handelspartnern und Lieferanten im Scope erfassen
- [ ] Scope-Dokument formal verabschieden und dokumentieren
- [ ] Scoping-Entscheidung vorab mit der Zertifizierungsstelle abstimmen

SCHRITT 02

Risikoanalyse durchführen

- [ ] Informationswerte identifizieren: ERP-Daten, Rezepturen, Produktionsdaten
- [ ] Bedrohungsszenarien bewerten (Ransomware, Lieferkettenangriff, Insiderrisiko)
- [ ] Risikobewertung nach definierter Methodik (Eintrittswahrscheinlichkeit × Schadenshöhe)
- [ ] Risikoakzeptanzschwelle durch Geschäftsführung formal freigeben lassen
- [ ] Ergebnisse im Risikoregister zentral dokumentieren und versionieren

SCHRITT 03

Richtlinien & ISMS-Leitlinie

- [ ] Informationssicherheitsleitlinie durch die Geschäftsführung unterzeichnen
- [ ] Mindestrichtlinien erstellen: Zugriffsrechte, Passwörter, mobile Geräte
- [ ] Richtlinie für Drittanbieter und Lieferanten (inkl. Transportdienstleister)
- [ ] Richtlinien intern kommunizieren und Kenntnisnahme dokumentieren
- [ ] Versionskontrolle für alle Dokumente einrichten und nachhalten

SCHRITT 04

Technische Maßnahmen

- [ ] Multi-Faktor-Authentifizierung für alle kritischen Systeme aktivieren
- [ ] Netzwerksegmentierung: IT von OT/ Produktionsanlagen trennen
- [ ] Backup-Konzept implementieren und Recovery-Tests dokumentieren
- [ ] Patch-Management und Schwachstellen-Scanning etablieren
- [ ] Penetrationstest oder Schwachstellenscan vor dem Audit einplanen

SCHRITT 05

Mitarbeiter schulen

- [ ] Awareness-Training für alle — inkl. Produktion und Logistik
- [ ] Phishing-Simulationen durchführen und Ergebnisse dokumentieren
- [ ] Sicherheitsverantwortliche in Schlüsselfunktionen benennen
- [ ] Schulungsnachweis für das Zertifizierungsaudit bereithalten
- [ ] Schulungsmaßnahmen jährlich wiederholen und aktualisieren

SCHRITT 06

Vorfallmanagement

- [ ] Incident-Response-Prozess definieren und Eskalationswege festlegen
- [ ] Meldefristen nach NIS2 (24h/72h) in den Prozess integrieren
- [ ] Kontakte zur zuständigen Behörde (BSI / Landesbehörde) hinterlegen
- [ ] Testlauf (Tabletop-Übung) durchführen und dokumentieren
- [ ] Lessons-learned-Prozess nach jedem Vorfall verankern

SECJUR

Ihre ISO 27001 Checkliste

Teil 2 von 2 — Lieferantenbewertung, Audit-Vorbereitung und Zertifizierung.

SCHRITT 07

Lieferanten bewerten

- [ ] Kritische Lieferanten und IT-Dienstleister identifizieren und priorisieren
- [ ] Sicherheitsanforderungen in Verträge und AVVs aufnehmen
- [ ] Jährliche Lieferantenbewertung etablieren (Fragebogen oder Audit)
- [ ] Cloud-Anbieter und SaaS-Dienste im Asset-Register erfassen
- [ ] Lieferantenregister pflegen und regelmäßig aktualisieren

SCHRITT 08

Business Continuity

- [ ] Kritische Prozesse und Recovery-Ziele (RTO/RPO) definieren
- [ ] Notfallplan für Produktionsausfall durch Cyberangriff dokumentieren
- [ ] Redundanzen für Kernsysteme (ERP, MES, QMS) prüfen und sicherstellen
- [ ] BCP einmal jährlich testen und Ergebnisse im ISMS festhalten
- [ ] Krisenteam benennen und Kontaktlisten aktuell halten

SCHRITT 09

Statement of Applicability

- [ ] Alle 93 Controls des Annex A auf Anwendbarkeit prüfen
- [ ] Für ausgeschlossene Controls: Begründung schriftlich dokumentieren
- [ ] SoA durch Geschäftsführung formal freigeben lassen
- [ ] SoA als zentrales Nachweisdokument für Auditoren bereithalten
- [ ] SoA versionieren und bei jedem Management Review aktualisieren

SCHRITT 10

Internes Audit

- [ ] Internen Auditor benennen oder externen Dienstleister beauftragen
- [ ] Alle ISMS-Kernbereiche nach ISO 19011 auditieren
- [ ] Abweichungen dokumentieren und Korrekturmaßnahmen einleiten
- [ ] Audit-Bericht der Geschäftsführung vorlegen (Management Review)
- [ ] Auditplan für die nächsten drei Jahre vorausplanen

SCHRITT 11

Zertifizierungsaudit bestehen

- [ ] Akkreditierte Zertifizierungsstelle auswählen und Stage-1-Audit planen
- [ ] Dokumentenpaket: Leitlinie, SoA, Risikoregister, Audit-Bericht bereitstellen
- [ ] Stage-2-Audit (Vor-Ort-Prüfung) erfolgreich bestehen
- [ ] Zertifikat erhalten — gültig 3 Jahre, jährliche Überwachungsaudits
- [ ] Zertifikat aktiv in Kundenkommunikation und Ausschreibungen einsetzen

TIPP FÜR FOUNDER & CEOS

Mit SECJUR DCO schneller zertifizieren

- [ ] Alle 93 Controls strukturiert in einer Compliance-Plattform abarbeiten
- [ ] Vorausgefüllte Richtlinienvorlagen für die Lebensmittelbranche nutzen
- [ ] Audit-Nachweise zentral dokumentieren — Auditoren erhalten direkten Zugang
- [ ] Expert:innen von SECJUR begleiten den gesamten Prozess bis zur Zertifizierung
- [ ] Überwachungsaudits und KVP-Zyklen direkt in der Plattform nachhalten

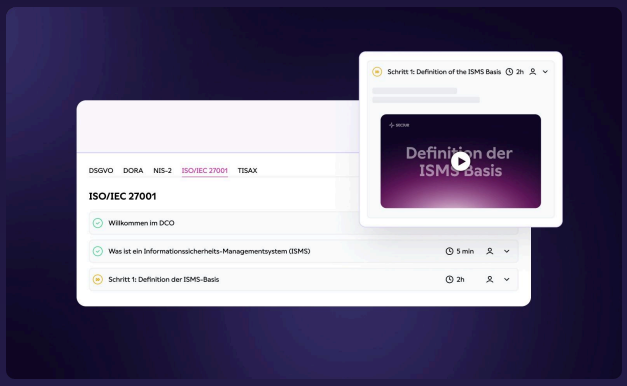
SECJUR

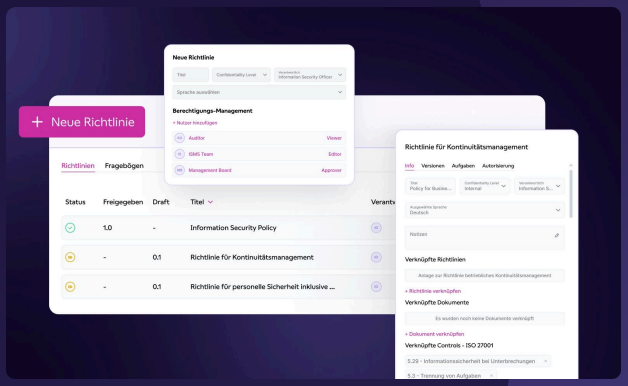
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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 automatisierten Compliance

"Mit SECJUR lassen sich alle NIS2-Anforderungen auf einer Plattform umsetzen. Dadurch konnten wir binnen einer Woche ein zentrales, skalierbares Richtliniensystem für die NIS2"

Dipl. Ing. Michael Dohr
Manager IT Security

Nordzucker

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR

yfood Trolli PETER KÖLLN demeter Nordzucker STERNWYWIOL Gruppe

www.secjur.com