SECJUR

ISO/IEC 27001 & DORA für FinTechs

Der praktische Fahrplan zum ISMS für Founder und CEOs im FinTech-Umfeld — von der BaFin-Anforderung bis zum Zertifikat.

Für FinTechs kommt der Anstoß meist von außen: Die BaFin erwartet Nachweise, Enterprise-Kunden schicken standardisierte Vendor-Assessments, und Investoren prüfen in der Tech-Due-Diligence systematisch Sicherheits-Governance. **ISO/IEC 27001** ist der internationale Standard, an dem sich diese Prüfungen orientieren — und deckt gleichzeitig bis zu **70 % der DORA-Anforderungen** ab. Statt zwei Compliance-Projekte parallel zu fahren, schafft ein strukturiertes ISMS die Basis für beides — und macht **Informationssicherheit nachweisbar**, statt sie bei jedem Kunden neu erklären zu müssen.

Wann ISO 27001 & DORA für FinTechs konkret wird:

TREIBER 01

Regulatorik & BaFin-Lizenz

Seit Januar 2025 gilt **DORA** für alle regulierten EU-Finanzunternehmen. BaFin-Anforderungen (BAIT) und Aufsichtsnachweise lassen sich mit einem ISMS **strukturiert und prüffest** erfüllen.

TREIBER 02

Fundraising & Investor-DD

VCs und strategische Investoren prüfen in der Tech-Due-Diligence systematisch **Datenzugriffe, Incident Response** und Security Governance. Ein laufendes ISMS reduziert rote Flaggen und **schützt die Bewertung**.

TREIBER 03

Enterprise-Sales & Onboarding

Banken und Corporates verlangen **ISO 27001-Zertifikate** oder detaillierte Vendor Assessments im Onboarding. Ein Zertifikat ersetzt Dutzende Fragebögen und **beschleunigt Enterprise-Deals** spürbar.

TREIBER 04

Operative Sicherheit & Resilienz

Smart Fintechs und vernetzte Zahlungssysteme vergrößern die **Angriffsfläche**. Ein ISMS bringt Asset-Transparenz, Incident Response und **Business Continuity** in genau diese Umgebung.

3–6 Monate

typische Zertifizierungszeit mit SECJUR Plattform & Expert:innen — statt 12+ Monate Eigenaufwand ohne Vorlage

~70 % DORA

der DORA-Anforderungen werden durch ISO 27001 Annex-A-Controls direkt abgedeckt — kein zweites Compliance-Projekt nötig

1 Zertifikat

löst Vendor-Fragebögen, Investoren-Due-Diligence & BaFin-Nachweise gleichzeitig — und öffnet Enterprise-Sales-Türen

SECJUR

Ihr Weg zum ISMS — Schritt 1 bis 6

Die ersten sechs Schritte schaffen das Fundament: Scope, Gap-Analyse, Dokumentation und eine belastbare Risikobasis für das regulierte FinTech-Umfeld.

SCHRITT 01

Scope & Kontext

- [ ] ISMS-Geltungsbereich **dokumentieren**
- [ ] Asset-Register **anlegen** (Systeme, Daten, Prozesse)
- [ ] Stakeholder und Anforderungen **erfassen**
- [ ] Regulatorischen Kontext aufnehmen (DORA, BAIT, PSD2)
- [ ] Managementsupport **formell einholen**

SCHRITT 02

Gap-Analyse durchführen

- [ ] Ist-Stand gegen ISO 27001:2022 Annex A **mappen**
- [ ] DORA-Anforderungen **parallel aufnehmen**
- [ ] Lücken nach Risiko und Regulatorik **priorisieren**
- [ ] Maßnahmen- und Zeitplan **ableiten**
- [ ] Umsetzungsbudget **freigeben lassen**

SCHRITT 03

ISMS-Dokumentation

- [ ] Informationssicherheitsleitlinie **erstellen**
- [ ] Sicherheitsziele und Kennzahlen **definieren**
- [ ] Rollen und Verantwortlichkeiten **zuweisen**
- [ ] Kern-Prozesse und Richtlinien **dokumentieren**
- [ ] Versionierung und Freigabeprozess **etablieren**
- [ ] Kommunikation an alle Mitarbeitenden **sicherstellen**

SCHRITT 04

Risiken bewerten

- [ ] Risikobewertungsmethode **festlegen**
- [ ] Assets, Bedrohungen und Schwachstellen **erfassen**
- [ ] Risikobehandlungsplan (RTP) **erstellen**
- [ ] Statement of Applicability (SoA) **erstellen**
- [ ] Risikoakzeptanz durch Management **bestätigen lassen**

SCHRITT 05

Maßnahmen & SoA

- [ ] Controls aus Annex A **auswählen**
- [ ] DORA-kritische Controls **priorisieren**
- [ ] Verantwortliche und Budget **zuordnen**
- [ ] Begründung je Control **festhalten**
- [ ] Ausnahmen und Restrisiken **dokumentieren**
- [ ] SoA regelmäßig **aktualisieren** und versionieren

SCHRITT 06

Leitlinien & Richtlinien

- [ ] Informationssicherheitsleitlinie **verabschieden**
- [ ] Zugriffs- und Passwortrichtlinien **festlegen**
- [ ] Regeln für Wechselmedien und Fernzugriff **etablieren**
- [ ] Dokumentenlenkung **etablieren**
- [ ] Klassifizierungsschema für Informationen **einführen**

SECJUR

DORA & BaFin — Schritt 7 bis 12

Die zweite Hälfte bringt DORA-Konformität und BaFin-Nachweise: ICT-Risikomanagement, Incident Reporting, Resilienztests und laufender Betrieb.

SCHRITT 07

ICT-Risikomanagement

- [ ] ICT-Risikomanagement-Framework **etablieren**
- [ ] Risikotoleranz auf Vorstandsebene **definieren**
- [ ] Business-Impact-Analyse (BIA) **durchführen**
- [ ] Recovery-Ziele (RTO/RPO) **festlegen** und testen
- [ ] Kritische ICT-Systeme **klassifizieren**
- [ ] Bedrohungsszenarien für FinTech-Umgebung **erfassen**

SCHRITT 08

Third-Party-Management

- [ ] Kritische Dienstleister und Partner **bewerten**
- [ ] Sicherheitsanforderungen **vertraglich verankern**
- [ ] Fernwartungszugänge **kontrollieren**
- [ ] Lieferanten **regelmäßig nachprüfen**
- [ ] Exit-Strategien für kritische Dienste **planen**
- [ ] Subunternehmer und Unterauftragnehmer **erfassen**

SCHRITT 09

Awareness & Notfallvorsorge

- [ ] Mitarbeitende **regelmäßig schulen**
- [ ] Incident-Response-Prozess **definieren**
- [ ] Meldewege (auch BaFin/DORA) **festlegen**
- [ ] Notfallübung in der Produktion **durchführen**
- [ ] Business-Continuity-Plan **testen**
- [ ] Schulungsnachweise **lückenlos dokumentieren**

SCHRITT 10

Internes Audit & Review

- [ ] Audit-Jahresprogramm mit Scope und Terminen **erstellen**
- [ ] Auditoren unabhängig benennen oder extern **beauftragen**
- [ ] Nichtkonformitäten erfassen und **priorisieren**
- [ ] Korrekturmaßnahmen einleiten und Wirksamkeit **prüfen**
- [ ] Audit-Berichte vollständig **dokumentieren**

SCHRITT 11

Managementbewertung

- [ ] Jährliche Review-Sitzung mit Geschäftsführung **durchführen**
- [ ] ISMS-Leistung, Auditberichte und Vorfälle **besprechen**
- [ ] Risiken und Chancen **aktualisiert bewerten**
- [ ] Verbesserungsmaßnahmen **beschließen** und zuordnen
- [ ] Sitzungsprotokoll als formellen Nachweis **dokumentieren**

SCHRITT 12 — ZIEL

Zertifizierungsaudit bestehen

- [ ] Stage-1-Audit: Dokumentenprüfung durch akkreditierten Auditor **bestehen**
- [ ] Stage-2-Audit: Nachweis der gelebten ISMS-Praxis vor Ort **liefern**
- [ ] Nichtkonformitäten **fristgerecht beseitigen**
- [ ] Zertifikat **erhalten** und kommunizieren
- [ ] Überwachungsaudits jährlich einplanen — Laufzeit 3 Jahre

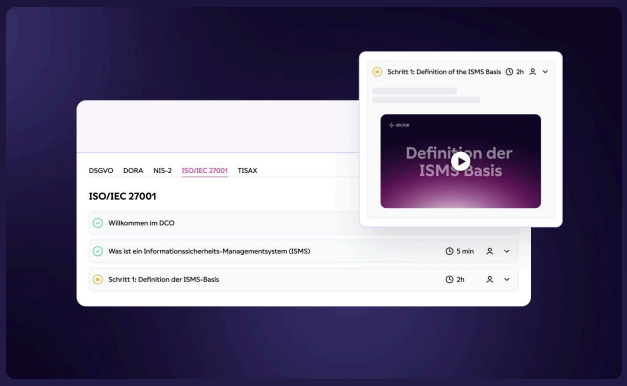
SECJUR

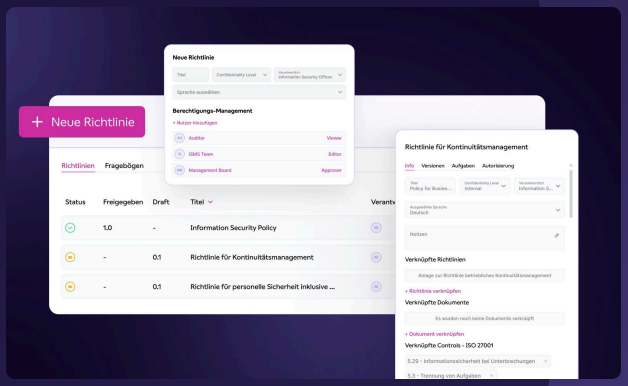
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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

vestlane NYALA AEQUITA BILTON BUILT ON VALUES Tomorrow EDEKABANK

www.secjur.com