NIS2 für die Finanzbranche

Der praktische Fahrplan für Fintechs und Finanz-Software-Anbieter: von der Betroffenheit bis zur Meldefähigkeit.

In der Finanzbranche greifen mehrere Regelwerke ineinander: Regulierte Banken und Versicherer fallen vorrangig unter DORA, **während viele Fintechs, Zahlungs- und Finanz-Software-Anbieter über NIS2 erfasst werden.** In Deutschland regelt das das **NIS2-Umsetzungsgesetz (NIS2UmsuCG).** Entscheidend ist die Frage, welches Regime greift und ob das eigene Unternehmen betroffen ist.

In diesen vier Situationen wird NIS2 für die Finanzbranche konkret:

BETROFFENHEIT & ABGRENZUNG

NIS2 oder DORA

- NIS2 und DORA grenzen sich nach Art der Einrichtung ab
- Fintechs, Payment- und Finanz-Software-Anbieter fallen oft unter NIS2
- Grobe Schwelle: rund 50 Beschäftigte oder 10 Mio. Euro Umsatz
- Saubere Einordnung ist der erste und wichtigste Schritt

RISIKOMANAGEMENT

Technische & organisatorische Pflichten

- Risikoanalyse, Zugriffskontrolle, Lieferkette, Backup, Notfallkonzept
- Sensible Finanz- und Zahlungsdaten: höchste Anforderungen
- Starke Verschlüsselung, Zugriffsschutz und Nachweisbarkeit
- Maßnahmen nachweisbar dokumentieren

MELDUNG & REGISTRIERUNG

Fristen sicher einhalten

- Erhebliche Vorfälle mehrstufig an die Behörde melden
- Erstmeldung sehr kurzfristig, danach Folgemeldungen
- Einrichtung fristgerecht registrieren
- Meldeprozess vorab aufsetzen, nicht erst im Ernstfall

GESCHÄFTSFÜHRUNG

Haftung der Leitungsebene

- GF muss Risikomaßnahmen billigen und überwachen
- Schulungspflicht für die Leitungsebene
- Verstöße können persönlich relevant werden
- Chefsache, gerade bei hoher Datensensibilität

NIS2 / DORA

Zwei Regime: die saubere Abgrenzung entscheidet über die geltenden Pflichten

Mehrstufig

Meldepflicht bei erheblichen Vorfällen: erst kurzfristig, dann Folgemeldungen

Chefsache

Leitungsorgane haften für Umsetzung und Überwachung der Risikomaßnahmen

SECJUR

NIS2-Readiness in 6 Schritten

Eine pragmatische Reihenfolge für Fintechs und Finanz-Software-Anbieter: von der Betroffenheitsprüfung bis zur Meldefähigkeit.

SCHRITT 01

Betroffenheit & Regime klären

- [ ] **NIS2 vs. DORA** für die eigene Einrichtung abgrenzen
- [ ] **Rolle** als digitaler Dienst oder Zahlungsanbieter prüfen
- [ ] **Einstufung** ableiten: wichtige vs. besonders wichtige Einrichtung
- [ ] **Betroffenheit** über Kundenlieferketten mitprüfen
- [ ] **Einordnung** bei Unsicherheit fachlich gegenprüfen und festhalten

SCHRITT 02

Registrierung vorbereiten

- [ ] **Zuständige Behörde** und Meldewege identifizieren
- [ ] **Kontaktstelle** und Verantwortliche benennen
- [ ] **Stammdaten** der Einrichtung zusammenstellen
- [ ] **Registrierungsfristen** im Kalender verankern
- [ ] **Änderungen** an Stammdaten laufend aktuell halten

SCHRITT 03

Risiken analysieren

- [ ] **Kritische Assets,** Zahlungs- und Datenflüsse erfassen
- [ ] **Bedrohungen** und Schwachstellen je Asset bewerten
- [ ] **Risiken** nach Eintritt und Schaden priorisieren
- [ ] **Maßnahmen** ableiten und Verantwortliche zuordnen
- [ ] **Ergebnis** als nachvollziehbares Risikoregister führen

SCHRITT 04

Maßnahmen umsetzen

- [ ] **Zugriffskontrolle,** MFA und starke Verschlüsselung etablieren
- [ ] **Backup-, Schlüssel-** und Patch-Prozesse aufsetzen
- [ ] **Zahlungs- und Datenflüsse** besonders absichern
- [ ] **Lieferkette** und Dienstleister-Risiken adressieren
- [ ] **Maßnahmen** als verbindliche Richtlinien dokumentieren

SCHRITT 05

Vorfälle & Meldung

- [ ] **Incident-Response-Prozess** definieren und testen
- [ ] **Meldekette** und Eskalationsstufen festlegen
- [ ] **Fristen** für Erst-, Folge- und Abschlussmeldung kennen
- [ ] **Vorlagen** für Erst- und Folgemeldungen vorbereiten
- [ ] **Verantwortlichkeiten** für den Ernstfall klären

SCHRITT 06

Leitung & Schulung

- [ ] **Geschäftsführung** in Risikomaßnahmen einbinden
- [ ] **Billigung** und Überwachung dokumentieren
- [ ] **Schulungen** für Leitung und Teams einplanen
- [ ] **Wirksamkeit** der Maßnahmen regelmäßig prüfen
- [ ] **Reviews** und Nachbesserungen fest verankern

SECJUR

Häufige Stolperfallen und Quick Wins

Was Fintechs und Finanz-Software-Anbieter bei NIS2 typischerweise unterschätzen, und womit sich früh Wirkung erzielen lässt. Links die Fallen, rechts die Hebel.

STOLPERFALLE 01

Regime verwechselt

- [ ] **NIS2 und DORA** ungeprüft gleichgesetzt, statt sauber abzugrenzen
- [ ] **Eigene Einrichtung** falsch eingeordnet
- [ ] **Falsches Regime** führt zu falschen oder doppelten Pflichten
- [ ] **Frühe, saubere Abgrenzung** spart später Hektik und Nacharbeit

QUICK WIN 01

Dokumentation zentralisieren

- [ ] **Richtlinien und Nachweise** an einem zentralen, auffindbaren Ort bündeln
- [ ] **Strukturiert und versioniert** ablegen, statt später mühsam zu sammeln
- [ ] **Verantwortliche** und Review-Zyklen je Dokument festlegen
- [ ] **Audits und Kundenfragen** lassen sich so spürbar schneller beantworten

STOLPERFALLE 02

Lieferkette ignoriert

- [ ] **Zahlungsdienstleister** und Cloud-Stack im Risiko unterschätzt
- [ ] **Sicherheitsanforderungen** nicht vertraglich mit Dienstleistern verankert
- [ ] **Keine Übersicht** über kritische Abhängigkeiten und Datenflüsse
- [ ] **Kundenanforderungen** schlagen vertraglich auf das Unternehmen durch

QUICK WIN 02

Synergien mit ISO 27001

- [ ] **Überlappung:** viele NIS2-Maßnahmen decken sich mit den ISO-27001-Controls
- [ ] **Ein ISMS** deckt NIS2, DORA und weitere Regime weitgehend gemeinsam ab
- [ ] **Bestehende Controls** gezielt auf die NIS2-Anforderungen mappen
- [ ] **Doppelarbeit** vermeiden und den Umsetzungsaufwand spürbar bündeln

STOLPERFALLE 03

Kein Meldeprozess

- [ ] **Meldekette** im Vorfall unklar, niemand weiß, wer zuerst zu informieren ist
- [ ] **Zuständigkeiten** und Vertretung für Meldungen vorab nicht benannt
- [ ] **Enge Meldefristen** werden im Ernstfall unter Zeitdruck verpasst
- [ ] **Vorbereitete Vorlagen** und ein klarer Ablauf entschärfen den Ernstfall

QUICK WIN 03

Vertrauen als Asset

- [ ] **Nachweisbare Sicherheit** stärkt Partner- und Kundenvertrauen
- [ ] **Compliance** wird vom Pflichtthema zum Wettbewerbsvorteil
- [ ] **Zertifikate und Nachweise** verkürzen Vendor- und Bank-Assessments
- [ ] **Von Unsicherheit** zu planbarer, nachweisbarer Readiness

SECJUR

Mit SECJUR zu 100 % NIS2-Compliance

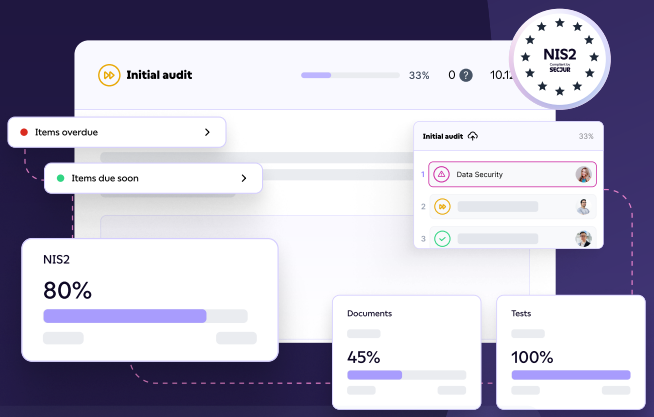
Mit der Durchsetzung der NIS2-Richtlinie in 2026 rücken zehntausende Unternehmen neu in den regulatorischen Fokus. Die Anforderungen an Informationssicherheit, Risikomanagement und Managementverantwortung steigen spürbar – ebenso wie die Erwartungen von Aufsichtsbehörden und Geschäftspartnern.

Mit dem Digital Compliance Office von SECJUR und unseren zertifizierten Expert:innen setzen Sie die Anforderungen der NIS2-Richtlinie strukturiert und effizient um. Bestehende Sicherheits- und Governance-Strukturen werden gezielt eingebunden und systematisch weiterentwickelt.

- Aufbau und Betrieb eines NIS2-konformen ISMS inkl. Risiko- und Incident-Management
- Klare Verantwortlichkeiten, Dokumentation und Nachweise für Behörden
- Profitieren Sie von der dedizierten Erfahrung unserer TÜV-geprüften Expert:innen

Reduzieren Sie manuellen Aufwand deutlich, gewinnen Transparenz über Ihren Compliance-Status und schaffen eine belastbare Grundlage für regulatorische Prüfungen und anspruchsvolle Kundenanforderungen.

Für unsere Bestandskunden bieten wir attraktive Konditionen, um frühzeitig Klarheit zu schaffen und NIS2-Readiness planbar umzusetzen.



→ **Jetzt informieren**

Mit SECJUR zu Informationssicherheitszertifizierungen:

“Dank Kundenvertrauen auf die Financial-Times-1000-Liste”

René Schlüß
Founder & Managing Director, reanmo

reanmo

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR

Masterplan.com · 1KOMMA5° · Tomorrow · deepset · yfood · vestlane

www.secjur.com