SECJUR

WHITEPAPER
2026

NIS2 & DORA · FINANZBRANCHE, FINTECH & FINANCIAL SOFTWARE

NIS2 & DORA für die Finanzbranche: zwei Gesetze, ein Fundament.

Kaum eine Branche ist so streng auf IT-Sicherheit reguliert wie die Finanzwelt. Für Finanzunternehmen gilt seit dem 17. Januar 2025 DORA, das speziellere Gesetz, das die NIS2-Pflichten in den IKT-Bereichen verdrängt. NIS2 gilt seit Dezember 2025 und bleibt maßgeblich fürs Umfeld und für IT- und Softwareanbieter, die selbst keine Finanzunternehmen sind. Dieses Whitepaper zeigt, wer unter welches Regime fällt, wo die beiden Gesetze sich überschneiden und wie sich beide mit einem einzigen, auditbereiten ISMS erfüllen lassen, statt in getrennten Projekten.

DORA NIS2 ISO 27001 SOC 2 DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

In der Finanzbranche ist Sicherheit doppelt reguliert.

DAS WICHTIGSTE IN KÜRZE

Zwei europäische Gesetze prägen die IT-Sicherheit der Finanzbranche. DORA, die Verordnung über die digitale operationale Resilienz, gilt seit dem 17. Januar 2025 unmittelbar für Finanzunternehmen. NIS2, in Deutschland über das NIS2UmsuCG seit dem 6. Dezember 2025 in Kraft, erfasst 18 Sektoren mit rund 29.500 Unternehmen.

Für Finanzunternehmen ist DORA das speziellere Gesetz. Es verdrängt die NIS2-Pflichten dort, wo es IKT-Risiken regelt, also beim Risikomanagement, der Vorfallmeldung und der Steuerung von IKT-Drittdienstleistern. Banken, Versicherer, Zahlungs- und E-Geld-Institute sowie viele FinTechs, die selbst Finanzunternehmen sind, arbeiten damit primär unter DORA. Für IT- und Softwareanbieter, die die Finanzbranche beliefern, ohne selbst Finanzunternehmen zu sein, bleibt NIS2 der maßgebliche Rahmen, ergänzt um die Anforderungen, die ihre Kunden aus der DORA-Drittparteienkette weiterreichen.

WARUM JETZT HANDELN

DORA gilt bereits ohne Übergangsfrist, und als besonders kritisch eingestufte IKT-Drittdienstleister stehen seit November 2025 unter direkter EU-Aufsicht. Parallel endete die NIS2-Registrierungsfrist beim BSI am 31. Juli 2026.

Der Druck kommt zusätzlich aus dem Markt. Jedes regulierte Institut muss seine Dienstleister nachweisbar steuern und reicht die Anforderungen vertraglich weiter. Wer die Nachweise nicht liefert, verliert den Zugang zu regulierten Kunden.

EIN FUNDAMENT FÜR BEIDE

DORA und NIS2 teilen dieselbe DNA: IKT-Risikomanagement, Vorfallmeldung, Drittparteiensteuerung und Resilienz. Wer ein ISMS nach ISO 27001 aufbaut, deckt einen Großteil beider Regime zugleich ab, statt jede Anforderung getrennt abzuarbeiten. Das gemeinsame Fundament trägt zusätzlich SOC 2 und die DSGVO.

Die folgenden Seiten ordnen ein, wer unter welches Gesetz fällt, welche Risiken die Branche konkret trägt, was DORA und NIS2 verlangen und wie ein Aufbau in wenigen Monaten auditbereit wird.

DORA GILT SEIT

17.01.2025

Unmittelbar für Finanzunternehmen, ohne Übergangsfrist, mit direkter EU-Aufsicht kritischer Anbieter.

NIS2 IN KRAFT

06.12.2025

Für das Umfeld und IT-Dienstleister, BSI-Registrierungsfrist am 31. Juli 2026 abgelaufen.

EIN FUNDAMENT

3 Standards

ISO 27001 deckt DORA, NIS2 und SOC 2 zu großen Teilen gemeinsam ab.

BRANCHENKONTEXT

Wer Banken beliefert, erbt ihre Regulierung.

Die Finanzbranche verarbeitet die sensibelsten Daten überhaupt und darf nur mit Dienstleistern arbeiten, die nachweisbar sicher sind. DORA und NIS2 geben diesem Anspruch seit 2025 einen scharfen gesetzlichen Rahmen.

Im Finanzsektor ist ein Vorfall nie nur ein IT-Problem, *sondern sofort ein Aufsichtsthema.*

DIE SENSIBELSTEN DATEN ÜBERHAUPT

Finanzsoftware verarbeitet Konto-, Zahlungs- und Identitätsdaten, oft in Echtzeit und in großer Menge. Diese Daten sind für Angreifer besonders wertvoll und für Aufsicht und Kunden besonders schützenswert.

Ein Vorfall ist hier nie nur ein IT-Problem, sondern sofort ein regulatorisches und ein Reputationsthema. Cloud-native gebaut, schnell skaliert und eng an die Kernsysteme der Banken angebunden: Genau diese Architektur macht die Branche leistungsfähig und zugleich zu einem lohnenden Ziel.

DORA UND DIE DRITTANBIETER-KETTE

Seit dem 17. Januar 2025 verlangt DORA von Finanzunternehmen, ihre IKT-Drittdienstleister vollständig in einem Informationsregister zu erfassen, vertraglich zu verpflichten und ihre Resilienz laufend zu überwachen. Als besonders kritisch eingestufte Anbieter stehen seit November 2025 unter direkter EU-Aufsicht.

Für einen Software- oder IT-Anbieter heißt das konkrete Vertragsklauseln: Sicherheitsanforderungen, Melde- und Audit-Rechte, Vorgaben zur Verfügbarkeit. Wer Banken beliefert, ist Teil dieser Kette, ob als Finanzunternehmen unter DORA oder als IT-Dienstleister unter NIS2.

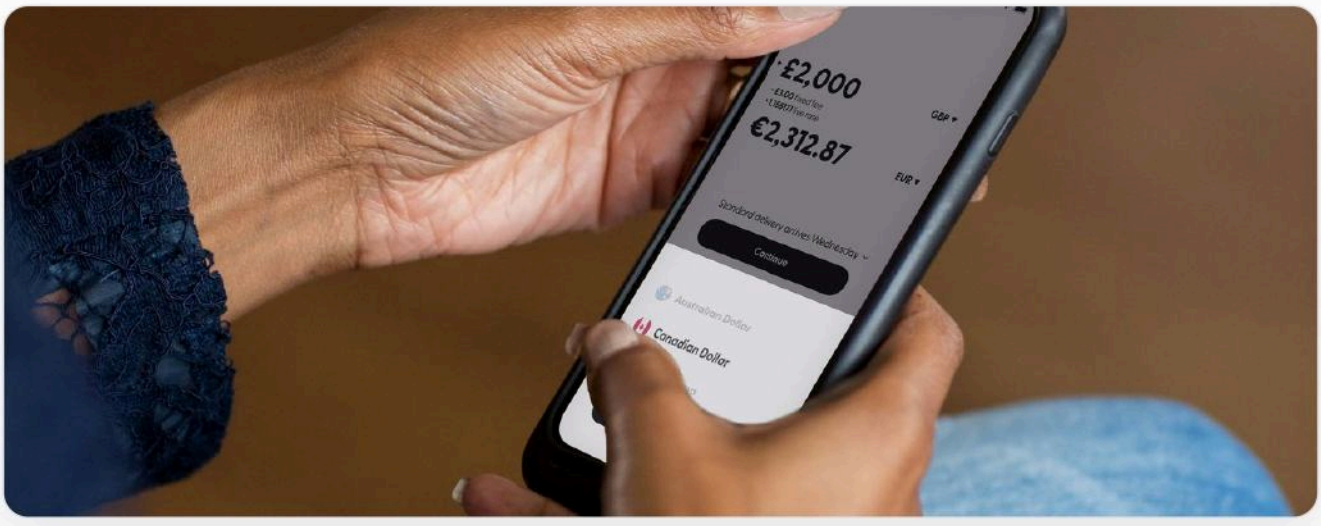
ZWEI REGIME, EINE REALITÄT

Finanzunternehmen erfüllen die IKT-Sicherheit über DORA, ihre nicht finanzregulierten IT- und Softwarepartner über NIS2. In der Praxis begegnen sich beide an derselben Schnittstelle: dem Vertrag zwischen Institut und Dienstleister. Ein anerkannter Nachweis ersetzt hier viele einzelne Prüfungen und verkürzt jede Auslagerungsprüfung.

WAS AUF DEM SPIEL STEHT

Im Finanzsektor wird Vertrauen in Verträgen und Aufsicht gemessen. Ein Vorfall kann nicht nur Kunden kosten, sondern den Zugang zum gesamten Markt, wenn Institute den Anbieter als Risiko einstufen.

Umgekehrt ist ein sauberer Nachweis bares Geld. Er sichert den Zugang zu regulierten Kunden, verkürzt Due-Diligence-Prüfungen und macht aus der Pflicht einen Vorsprung. Sicherheit ist hier die Lizenz zum Geschäft.



HERAUSFORDERUNGEN

Warum NIS2 und DORA die Finanzbranche besonders fordern.

Die Anforderungen gelten unabhängig von der Größe. Im Finanzumfeld liegt die Latte aber höher, und Tempo trifft auf strenge Kontrolle. Sechs Eigenheiten machen die Umsetzung speziell, und für jede gibt es einen pragmatischen Umgang.

HÖCHSTE REGULATORISCHE LATTE

Kein anderer Kunde prüft so genau wie eine Bank. Sicherheitsfragebögen sind länger, Audit-Rechte härter, und DORA verlangt nachweisbare operationale Resilienz. Die gute Nachricht: Ein ISMS nach ISO 27001 deckt einen Großteil dieser Erwartungen strukturiert ab und schafft ein Fundament, das Prüfungen standhält, statt auf jede Anforderung einzeln zu reagieren. Was bei einem gewöhnlichen Enterprise-Kunden genügt, ist im Finanzumfeld oft erst der Anfang.

OPERATIVE RESILIENZ NACHWEISEN

Institute brauchen ihre Systeme rund um die Uhr. DORA verlangt, dass auch Dienstleister Ausfälle übersteht und schnell wieder anläuft. Getestete Wiederanlaufpläne, definierte Wiederanlaufzeiten und Business Continuity stehen deshalb besonders im Fokus, samt regelmäßiger Tests statt bloßer Konzepte auf Papier. Institute verlangen konkrete Wiederanlaufzeiten und prüfen, ob sie im Test auch wirklich erreicht werden.

TEMPO GEGEN KONTROLLE

Die Branche lebt von schnellen Releases. Strenge Change- und Zugriffskontrollen wirken dem zunächst entgegen. Der Ausweg liegt in Automatisierung und Verhältnismäßigkeit: Kontrollen in die CI/CD-Pipeline integrieren, Nachweise automatisch erzeugen und den Umfang an Größe und Risiko ausrichten. Wird das ISMS zu schwer aufgesetzt, bremst es die Produktentwicklung aus, statt sie abzusichern.

PRIVILEGIERTE ZUGÄNGE UND ZAHLUNGSDATEN

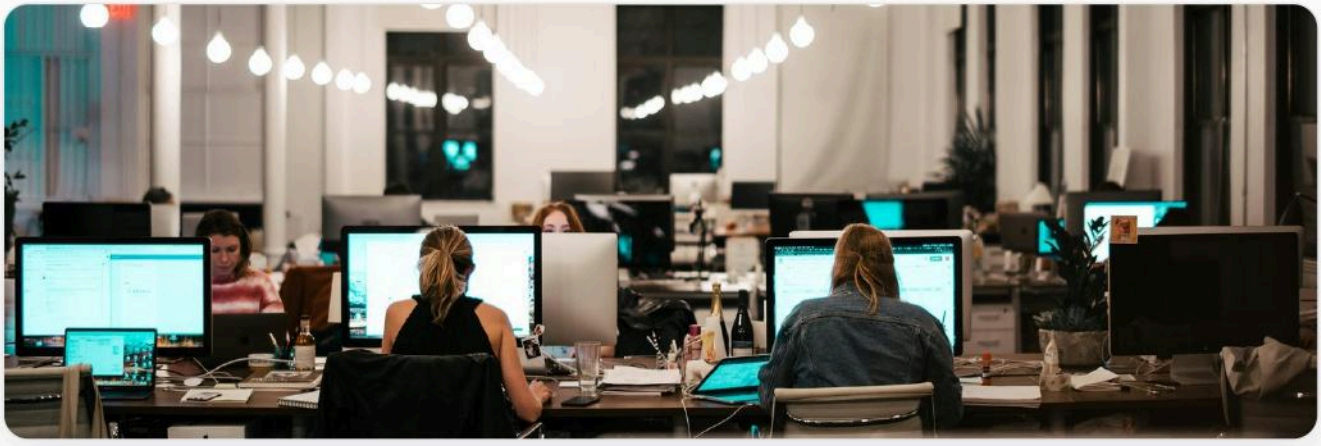
Wer an Kernbankensysteme angebunden ist und Zahlungsdaten verarbeitet, verwaltet hochsensible Zugänge. Diese müssen streng vergeben, getrennt und protokolliert werden. Bei Kartendaten kommt häufig PCI DSS als zusätzliche Anforderung hinzu. Jeder Zugang gehört nach Projektende konsequent entzogen, damit keine verwaisten Rechte zurückbleiben.

DRITTANBIETER UND KONZENTRATION

Auch Finanzunternehmen stützen sich selbst auf Cloud- und SaaS-Dienste, über die Finanzdaten laufen. Aufsicht und Kunden achten auf Konzentrationsrisiken und Sub-Dienstleister. Eine dokumentierte Lieferantensteuerung mit Anforderungen und Nachweis ist unter DORA wie NIS2 ein Kernpunkt jeder Prüfung.

DOPPELREGULIERUNG OHNE DOPPELARBEIT

Wer sowohl als Finanzunternehmen unter DORA als auch in Randbereichen unter NIS2 fällt, riskiert zwei getrennte Projekte. Weil beide Regime denselben Kern teilen, lässt sich das vermeiden: ein Aufbau, der beide Nachweise zugleich bedient, statt sie doppelt zu pflegen.



BEDROHUNGSLAGE & RISIKEN

Wo die Finanzbranche konkret angreifbar ist.

Die Risiken hängen an sensiblen Finanzdaten, an der Anbindung zu Banken und an der hohen Verfügbarkeitserwartung. Fünf Szenarien tauchen immer wieder auf. Sie alle haben eine Gemeinsamkeit: Aus einem technischen Vorfall wird schnell ein regulatorisches und vertragliches Problem.

1 · ABFLUSS VON ZAHLUNGS- UND KONTODATEN

Der teuerste Ernstfall. Werden Konto-, Karten- oder Identitätsdaten abgegriffen, folgen Betrug, Meldepflichten und ein massiver Vertrauensverlust bei den belieferten Instituten. Verschlüsselung, strenge Zugriffskontrolle und Protokollierung sind hier die zentralen Hebel. Hinzu kommen Melde- und Nachweispflichten gegenüber Aufsicht und Kunden, die nur mit lückenloser Protokollierung fristgerecht zu erfüllen sind. Ein einziger Abfluss kann Meldeketten gegenüber mehreren belieferten Instituten zugleich auslösen.

2 · AUSFALL DER OPERATIVEN RESILIENZ

Institute erwarten nahezu durchgehende Verfügbarkeit. Ein längerer Ausfall trifft unmittelbar deren Geschäft und löst unter DORA Melde- und Nachweispflichten aus. Getestete Wiederanlaufpläne und Business Continuity entscheiden, wie schnell der Betrieb zurückkehrt. Verlangt werden konkrete Wiederanlaufzeiten und regelmäßige Tests, nicht bloß ein Konzept. Regelmäßige Übungen zeigen vorab, wo der Wiederanlauf im Ernstfall noch hakt.

3 · GESCHEITERTE AUFSICHTSPRÜFUNG

Ein konkretes Geschäftsrisiko. Scheitert ein Anbieter an der Auslagerungs- oder DORA-Prüfung eines Instituts, steht der Vertrag auf dem Spiel, oft das Kerngeschäft. Ein vorliegendes Zertifikat verschiebt das Gespräch vom Ob zur Umsetzung und verkürzt die Prüfung erheblich, weil das Institut auf einen anerkannten Nachweis zurückgreift. So wird aus einer langwierigen Auslagerungsprüfung ein kurzer Abgleich, und der Vertrag kommt schneller zustande.

4 · ANGRIFF ÜBER DIE LIEFERKETTE

Finanzunternehmen und ihre Anbieter stützen sich auf weitere Dienste. Ein kompromittierter Sub-Dienstleister oder ein manipuliertes Update wird zum Einstieg in sensible Umgebungen. Lieferantensteuerung und sichere Entwicklung begrenzen dieses Risiko. Aufsicht und Kunden achten dabei besonders auf Konzentrationsrisiken bei gemeinsamen Cloud-Diensten. Ein aktuelles Verzeichnis aller Sub-Dienstleister ist die Grundlage, um solche Ketten überhaupt zu überblicken.

5 · MISSBRAUCH PRIVILEGIERTER ZUGÄNGE

Zugänge zu Kernbankensystemen und Produktivumgebungen sind das lohnendste Ziel. Werden Zugangsdaten abgegriffen oder nach Projektende nicht entzogen, steht Angreifern viel offen. Privileged-Access-Management, Mehrfaktor-Anmeldung und Protokollierung schließen diese Tür. Gerade bei Fernzugängen externer Dienstleister ist die lückenlose Nachvollziehbarkeit jedes Zugriffs entscheidend. Sie macht ungewöhnliche Zugriffe früh sichtbar und ist im Prüffall der entscheidende Nachweis gelebter Kontrolle. Gerade externe Fernzugänge brauchen zusätzlich feste Zeitfenster und eine Mehrfaktor-Anmeldung.

REGULATORISCHE PFLICHTEN

Was DORA und NIS2 konkret verlangen.

Zwei Regime, ein Kern. DORA regelt die IKT-Sicherheit der Finanzunternehmen, NIS2 das Umfeld und die nicht finanzregulierten IT-Anbieter. Fünf Bausteine muss jeder betroffene Anbieter kennen.

WER UNTER DORA FÄLLT, WER UNTER NIS2

Finanzunternehmen wie Banken, Versicherer, Zahlungs- und E-Geld-Institute, Wertpapierfirmen und Krypto-Dienstleister fallen unter DORA. Als speziellere Regelung verdrängt DORA die NIS2-Pflichten dort, wo es IKT-Risiken regelt. IT- und Softwareanbieter, die die Finanzbranche beliefern, ohne selbst Finanzunternehmen zu sein, fallen unter NIS2, sofern sie die Schwellenwerte erreichen (ab 50 Beschäftigte oder 10 Mio. Euro), und zusätzlich über die DORA-Drittparteienkette ihrer Kunden. In Zweifelsfällen lohnt eine kurze rechtliche Einordnung, bevor der Aufbau startet.

DORA · IKT-RISIKOMANAGEMENT

Finanzunternehmen brauchen einen dokumentierten IKT-Risikomanagementrahmen: Identifizierung der Assets, Schutz und Erkennung, Backup und Wiederherstellung sowie eine klare Governance. Die Leitung trägt die Verantwortung ausdrücklich. Ein ISMS nach ISO 27001 liefert genau diese Struktur und deckt den Rahmen weitgehend ab. Der Rahmen ist regelmäßig zu überprüfen und an neue Bedrohungen anzupassen.

DORA · VORFALLMELDUNG UND RESILIENZTESTS

Schwerwiegende IKT-Vorfälle sind gestuft an die zuständige Aufsicht zu melden, mit Erst-, Zwischen- und Abschlussmeldung. Hinzu kommt das regelmäßige Testen der digitalen operationalen Resilienz, für bedeutende Institute bis hin zu bedrohungsorientierten Penetrationstests. Geübte Abläufe und getestete Wiederanlaufpläne sind hier Pflicht. Die Fristen laufen ab Kenntnis des Vorfalls, ein vorbereiteter Ablauf spart im Ernstfall wertvolle Zeit.

DORA · DRITTPARTEIEN UND KONZENTRATION

Institute müssen ihre IKT-Drittdienstleister im Informationsregister führen, vertraglich verpflichten und laufend überwachen, mit Blick auf Konzentrationsrisiken. Als kritisch eingestufte Anbieter stehen unter direkter EU-Aufsicht. Für Dienstleister heißt das: Der eigene Nachweis wird zur Eintrittskarte in die Kette. Auch die eigenen Sub-Dienstleister gehören dokumentiert, damit die Kette lückenlos bleibt.

NIS2 · WAS ZUSÄTZLICH GILT, PLUS SANKTIONEN

Für IT-Anbieter außerhalb der DORA-Definition gelten die NIS2-Pflichten: angemessene Maßnahmen nach §30, die gestufte Meldung an das BSI (24 Stunden, 72 Stunden, ein Monat) nach §32 und die nicht delegierbare Leitungsverantwortung nach §38. Verstöße kosten unter NIS2 bis zu 10 Mio. Euro oder 2 % des Umsatzes, unter DORA drohen eigene, empfindliche Aufsichtsmaßnahmen. Ein dokumentierter, gelebter Prozess ist im Prüffall die beste Verteidigung. Wer beide Regime aus einem Aufbau bedient, hält die Nachweise konsistent und den Aufwand niedrig.

UMSETZUNG IN DER PRAXIS

In sechs Schritten zu einem Nachweis für beide.

Die Umsetzung lässt sich planen. Diese Reihenfolge baut auf der starken Technikbasis der Branche auf und bedient DORA und NIS2 aus einem Aufbau. Realistisch führt der Weg in wenigen Monaten zu einem auditbereiten Stand.

Ein ISMS, das einmal steht, trägt ISO 27001, DORA und NIS2 zugleich. *Ein Fundament, mehrere Nachweise.*

1 · REGIME UND GELTUNGSBEREICH KLÄREN

Zuerst feststellen, ob das Unternehmen als Finanzunternehmen unter DORA fällt, als IT-Anbieter unter NIS2 oder über die Drittparteienkette gebunden ist. Den Scope auf die Plattform und die Dienste schneiden, die Institute tatsächlich prüfen. Diese Einordnung ist die Grundlage für alles Weitere und gehört in die Unterlagen der Leitung.

2 · FÜHRUNG UND LEITLINIE

Die Geschäftsführung verabschiedet die Sicherheitsleitlinie, benennt eine verantwortliche Person und stellt Ressourcen bereit. DORA wie NIS2 machen Sicherheit ausdrücklich zur nicht delegierbaren Leitungsaufgabe. In technikgetriebenen Teams ist dieser Schritt schnell erledigt, wenn die Spitze dahintersteht.

3 · ASSETS UND RISIKEN ERFASSEN

Ein Inventar aufbauen, von der Plattform über Bank-Anbindungen bis zu den genutzten Cloud- und SaaS-Diensten. Risiken rund um Finanzdaten, Verfügbarkeit und Zugänge bewerten und nach Wirkung priorisieren. Eine gute Analyse macht den Aufwand planbar und speist zugleich das DORA-Informationsregister.

4 · MASSNAHMEN UMSETZEN

Mit den wirksamsten Hebeln beginnen: Business Continuity, Zugriffs- und Privileged-Access-Management, sichere Entwicklung und Lieferantenanforderungen. Wo möglich, Kontrollen in die Pipeline integrieren und Nachweise automatisch erzeugen. Jede Maßnahme so dokumentieren, dass sie im Audit Bestand hat.

5 · MELDE- UND TESTPROZESSE AUFBAUEN

Die Meldeketten für DORA und, wo einschlägig, für NIS2 einrichten, Zuständigkeiten klären und die Wiederanlaufpläne testen. Im Ernstfall zählt jede Stunde, und nur geübte Abläufe halten die Fristen. Regelmäßige Resilienztests sind unter DORA Pflicht, nicht Kür.

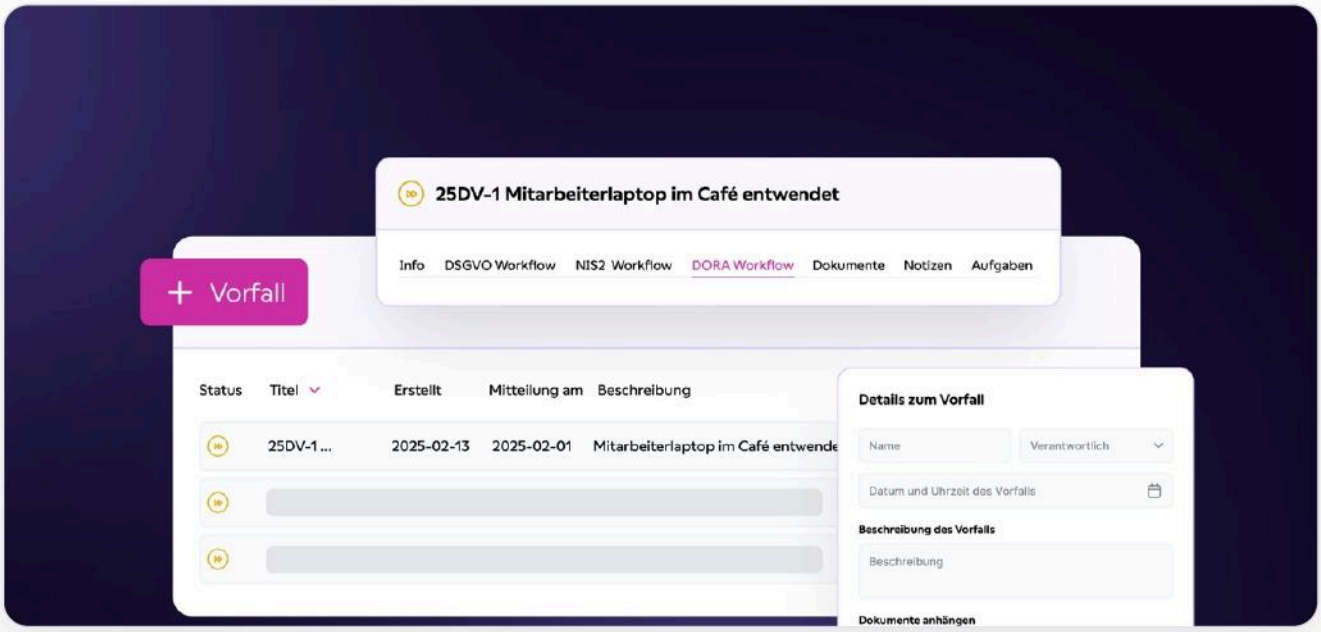
6 · PRÜFEN, VERBESSERN, NACHWEISEN

Internes Audit und Managementbewertung prüfen die Wirksamkeit, Korrekturmaßnahmen schließen Lücken. Diese Schleife deckt sich mit der laufenden Überwachung, die DORA verlangt, und ist zugleich die Generalprobe für jede Bank-Prüfung. Wer SOC 2 oder ein ISO-Zertifikat ergänzt, baut auf demselben Fundament auf.

WIE SECJUR ES EINFACH MACHT

Zwei Gesetze, ein auditbereites ISMS.

Das Digital Compliance Office (DCO) führt Finanzunternehmen und ihre IT-Anbieter durch DORA und NIS2 zugleich: Risiken, Maßnahmen, Meldeprozesse, Drittparteienregister und Nachweise an einem Ort, mehrere Frameworks parallel. Statt monatelanger Beratung arbeiten Sie in einer Oberfläche, gehostet in Deutschland und selbst nach ISO 27001 zertifiziert. Teams berichten von bis zu 50 Prozent schnellerer Umsetzung gegenüber klassischer Beratung.



DORA & Resilienz

Module für IKT-Risikomanagement, Wiederanlaufpläne und Resilienztests, genau die Nachweise, die Aufsicht und Institute unter DORA verlangen.

Drittparteien & Register

Lieferantensteuerung und ein Informationsregister, das die DORA-Drittparteienkette und die NIS2-Lieferkettenpflicht gemeinsam bedient.

Mehrere Frameworks

DORA, NIS2, ISO 27001 und SOC 2 laufen auf einem ISMS, gemeinsame Maßnahmen werden nur einmal gepflegt statt viermal.

SO LÄUFT DIE EINFÜHRUNG

Der Einstieg ist schlank. Sie klären das Regime und den Geltungsbereich, das DCO führt durch jede Anforderung, und wo eine Expertin nötig ist, schalten wir sie zu. Sie entscheiden, das System dokumentiert im Hintergrund. So wird aus vorhandener Technik in Wochen ein auditbereites ISMS, statt in Quartalen.

Konkret beginnt es mit einer geführten Aufnahme. Das DCO fragt Betroffenheit, Assets, Zugänge und bestehende Maßnahmen ab und leitet daraus die offenen Punkte für DORA und NIS2 ab. Jeder Schritt ist mit einer Vorlage hinterlegt, sodass niemand vor einem leeren Blatt sitzt.

Wo es schnell gehen muss, arbeitet das Team die wirksamsten Maßnahmen zuerst ab und verteilt den Rest planbar. Der Fortschritt bleibt jederzeit sichtbar, auch im laufenden Produktgeschäft.

EIN FUNDAMENT, MEHRERE NACHWEISE

Weil sich DORA, NIS2, ISO 27001 und SOC 2 weitgehend überschneiden, deckt das DCO sie gemeinsam ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, von Microsoft 365 bis zur Cloud, sodass das ISMS auch im schnellen Produktgeschäft aktuell bleibt.

Für ein Finanzunternehmen heißt das weniger Doppelarbeit. Der DORA-Nachweis lässt sich mit wenigen Ergänzungen zur ISO-27001-Zertifizierung oder zum SOC-2-Testat ausbauen, statt jedes Mal von vorn zu beginnen.

Und weil die Belege aktuell bleiben, ist das Unternehmen für die nächste Bank-Prüfung oder Aufsichtsanfrage vorbereitet, ohne kurzfristig Unterlagen zusammensuchen zu müssen. Aus einer Pflicht wird so ein dauerhafter Vorteil.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen arbeiten mit SECJUR.

FinTechs, Zahlungsdienstleister, Banken, Versicherer und ihre Software-Häuser erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus dem FinTech-Umfeld:

„Dank Kundenvertrauen auf die *Financial-Times-1000-Liste.*"

René Schlüß
Founder & Managing Director, reanmo

REFERENZEN AUS FINTECH, FINANCIAL SOFTWARE UND PAYMENTS

vestlane · NYALA · AEQUITA · BILTON · Tomorrow · EDEKABANK

AUDIT-ERFOLG
100%
Erfolgsquote in bisherigen Zertifizierungsaudits.

ZEITERSPARNIS
50%
Weniger Aufwand gegenüber klassischer Beratung.

INTEGRATIONEN
60+
Native API-Anbindungen, von Microsoft 365 bis GitHub.

STANDARDS
10+
Frameworks parallel abgedeckt, ohne Doppelarbeit.

WARUM DIE FINANZBRANCHE SECJUR WÄHLT

Der Reiz liegt in der Geschwindigkeit. Statt monatelanger Beratung führt ein klarer Pfad durch jede Anforderung, mit Vorlagen, die DORA, NIS2, ISO 27001 und SOC 2 zugleich bedienen. Das Team bleibt beim Produkt, die Compliance entsteht parallel.

Nachweise wachsen dabei ohne zusätzliche Personaldecke. Über native Integrationen zieht das DCO Belege automatisch aus den Systemen, mit denen ohnehin gearbeitet wird, sodass Geschäftsführung, Technik und Compliance an einer Quelle arbeiten statt an verstreuten Tabellen.

Wo Fachwissen fehlt, schalten sich Expertinnen und Experten gezielt zu, statt ein dauerhaftes Beratungsmandat zu verlangen. Das hält die Kosten im Rahmen und die Kontrolle im Haus, gerade in schnell wachsenden Teams.

Und die Plattform denkt in der Realität eines regulierten Produktgeschäfts. Sie priorisiert die Maßnahmen mit der größten Wirkung und macht auf einen Blick sichtbar, was noch offen ist, damit die Umsetzung planbar bleibt.

MEHR ALS EINE PFLICHTÜBUNG

Am Ende steht nicht nur ein erfülltes Gesetz, sondern ein Anbieter, der seine Resilienz nachweist, seine Lieferkette steuert und jede Bank-Prüfung souverän besteht. Genau das gewinnt regulierte Kunden und hält sie.

Ein gelebtes ISMS macht Sicherheit vom Vertriebshindernis zum Argument. Due-Diligence-Fragen sind in Stunden beantwortet, Bank-Audits verlieren ihren Schrecken, und Partner sehen belegt, dass ihr Anbieter reguliert und stabil ist.

Ein sauberer Nachweis wirkt weit über die Aufsicht hinaus. Er verkürzt die Prüfungen großer Kunden, entkräftet Einwände in Ausschreibungen und verschafft einen Vorsprung gegenüber Wettbewerbern, die den Nachweis erst noch aufbauen müssen.

Und der Aufwand bleibt einmalig. Was heute für DORA und NIS2 entsteht, trägt morgen die ISO-27001-Zertifizierung, das SOC-2-Testat und die nächste Finanzierungsrunde. Sicherheit wird so zum festen Bestandteil der Art, wie das Unternehmen arbeitet.

SECJUR

Mit SECJUR zu 100 % NIS2-Compliance

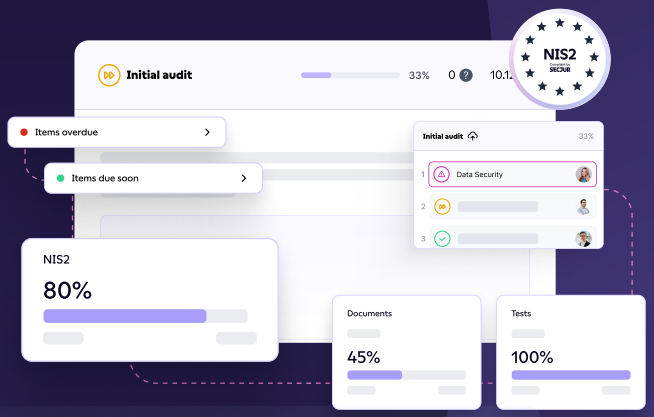
Mit der Durchsetzung der NIS2-Richtlinie in 2026 rücken zehntausende Unternehmen neu in den regulatorischen Fokus. Die Anforderungen an Informationssicherheit, Risikomanagement und Managementverantwortung steigen spürbar – ebenso wie die Erwartungen von Aufsichtsbehörden und Geschäftspartnern.

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