SECJUR

WHITEPAPER
2026

ISO 27001 · FINTECH & FINANCIAL SOFTWARE

ISO 27001 für FinTechs: *Sicherheit auf Banken-Niveau.*

Wer Software an Banken, Versicherer und Zahlungsdienstleister verkauft, erbt deren Regulierung. Seit DORA im Januar 2025 gilt, stehen IT-Drittanbieter des Finanzsektors unter besonderer Beobachtung, und jedes Institut muss seine Dienstleister nachweisbar steuern. ISO 27001 ist der anerkannte Beleg, dass ein FinTech die Sicherheit liefert, die seine regulierten Kunden brauchen. Dieses Whitepaper zeigt, warum der Standard für Software-Provider im Finanzsektor zur Geschäftsgrundlage wird und wie ein zertifizierungsreifes ISMS entsteht.

ISO 27001 · DORA · SOC 2 · PCI DSS · DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Im Finanzsektor verkaufen Sie *Software und Vertrauen.*

DAS WICHTIGSTE IN KÜRZE

ISO/IEC 27001 ist der international führende Standard für Informationssicherheits-Managementsysteme (ISMS). Anders als DORA ist er freiwillig. Für FinTech-Softwareanbieter ist er trotzdem fast verpflichtend, weil ihre Kunden, Banken und Versicherer, streng reguliert sind und ihre Anforderungen an die Dienstleister weitergeben. Das Zertifikat ist der unabhängige Nachweis, dass diese Anforderungen erfüllt sind.

Ein ISMS ist dabei kein reines IT-Thema. Es ist ein Satz aus klaren Regeln, Verantwortlichkeiten und Nachweisen, der zeigt, dass ein Anbieter mit den sensibelsten Daten überhaupt, Konto-, Zahlungs- und Identitätsdaten, sorgfältig umgeht.

Weltweit sind über 70.000 Organisationen nach ISO 27001 zertifiziert, mit deutlich steigender Tendenz. Seit dem 31. Oktober 2025 gilt ausschließlich die Fassung von 2022; die ältere Version :2013 ist mit dem Ende der Übergangsfrist ausgelaufen.

WARUM JETZT HANDELN

Der regulatorische Druck ist seit Anfang 2025 deutlich gestiegen. Mit DORA, das seit dem 17. Januar 2025 gilt, müssen Finanzinstitute ihre IT-Drittanbieter in einem Register führen, vertraglich verpflichten und laufend überwachen. Kritische Anbieter unterliegen seit November 2025 sogar einer direkten EU-Aufsicht. Wer Banken beliefert, ist Teil dieser Kette.

Für einen Software-Provider heißt das: Der Kunde muss nachweisen, dass sein Dienstleister sicher ist, und gibt diese Pflicht weiter. ISO 27001 ist die strukturierte Antwort, die einen Großteil der DORA- und Auslagerungsanforderungen abdeckt. Dieses Whitepaper ordnet ein, was die Norm verlangt und wie der Weg dorthin aussieht.

WOFÜR SICH DER SCHRITT LOHNT

Drei Signale sprechen klar für ISO 27001: Banken machen das Zertifikat zur Vergabebedingung, Sie erhalten Auslagerungs- und DORA-Klauseln samt Audit-Rechten in Verträgen, oder Sie verarbeiten Zahlungs- und Kontodaten. Trifft eines zu, ist das Zertifikat selten eine Frage des Ob, sondern des Wann.

Die gute Nachricht: Ein einmal aufgebautes ISMS trägt mehrere Nachweise zugleich. ISO 27001 als Fundament deckt einen Großteil von DORA und SOC 2 mit ab, statt für jede Anforderung von vorn zu beginnen.

WELTWEIT ZERTIFIZIERT

70.000+

Organisationen sind nach ISO 27001 zertifiziert, mit klar steigender Tendenz.

DORA GILT SEIT

2025

Seit 17.01.2025 stehen IT-Drittanbieter des Finanzsektors unter verschärfter Aufsicht.

KONTROLLEN

93

Maßnahmen im Annex A, in vier Gruppen von organisatorisch bis technisch.

BRANCHENKONTEXT

Wer Banken beliefert, *erbt ihre Regulierung.*

FinTech-Softwareanbieter sitzen an einer hochregulierten Stelle: Ihre Kunden unterliegen BaFin-Aufsicht und DORA und dürfen nur mit Dienstleistern arbeiten, die nachweisbar sicher sind. ISO 27001 macht diesen Nachweis auf einen Blick möglich, statt ihn in jedem Vertrag neu zu verhandeln.

Die Bank haftet für ihre Dienstleister. *Also prüft sie jeden einzelnen.*

DIE SENSIBELSTEN DATEN ÜBERHAUPT

FinTech-Software 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 FinTechs leistungsfähig und zugleich zu einem lohnenden Ziel.

DORA UND DIE DRITTANBIETER-KETTE

Seit dem 17. Januar 2025 verlangt DORA von Finanzinstituten, ihre IT-Drittanbieter vollständig zu erfassen, vertraglich zu verpflichten und ihre Resilienz laufend zu überwachen. Als besonders kritisch eingestufte Anbieter stehen seit November 2025 unter direkter EU-Aufsicht.

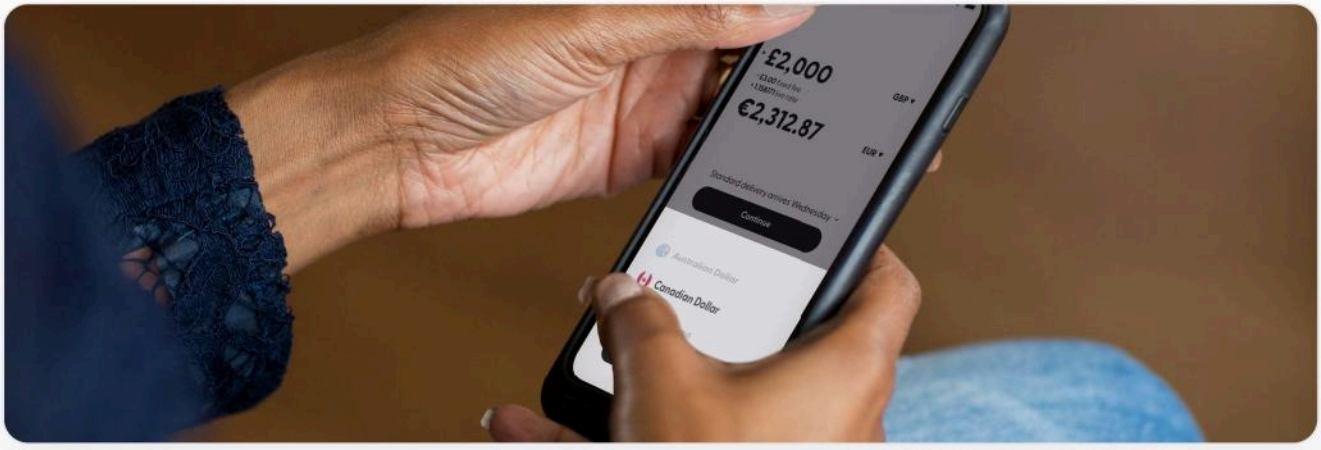
Für den Software-Provider bedeutet das konkrete Vertragsklauseln: Sicherheitsanforderungen, Melde- und Audit-Rechte, Vorgaben zur Verfügbarkeit. Ein ISMS nach ISO 27001 ist die strukturierte Grundlage, um diese Erwartungen verlässlich zu erfüllen.

AUSLAGERUNG UNTER BAFIN-AUFSICHT

Schon vor DORA galt: Lagert eine Bank IT an einen Dienstleister aus, bleibt sie verantwortlich und muss den Anbieter steuern und prüfen. Die aufsichtlichen Anforderungen an Auslagerungen verlangen genau die Kontrollen, die ein ISMS ohnehin dokumentiert. Das Zertifikat ersetzt viele einzelne Nachweise.

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. Sicherheit ist hier die Lizenz zum Geschäft.



HERAUSFORDERUNGEN

Warum ISO 27001 FinTechs *besonders fordert.*

Die Anforderungen der Norm gelten unabhängig von der Branche. Im Finanzsektor liegt die Latte aber höher, und Tempo trifft auf strenge Kontrolle. Fünf Eigenheiten machen die Umsetzung speziell.

HÖCHSTE REGULATORISCHE LATTE

Kein anderer Kunde prüft so genau wie eine Bank. Sicherheitsfragebögen sind länger, Audit-Rechte härter, und DORA verlangt nachweisbare operative Resilienz. Was bei einem normalen Enterprise-Kunden genügt, ist hier oft erst der Anfang.

Die gute Nachricht: ISO 27001 deckt einen Großteil dieser Erwartungen strukturiert ab. Statt auf jede Anforderung einzeln zu reagieren, schafft das ISMS ein Fundament, das Prüfungen und Audits standhält.

TEMPO GEGEN KONTROLLE

FinTechs leben von schnellen Releases. Strenge Change- und Zugriffskontrollen wirken dem zunächst entgegen. Wird das ISMS zu schwer aufgesetzt, bremst es die Produktentwicklung aus.

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 (Kap. 6.1, Annex A 8.25 bis 8.32).

OPERATIVE RESILIENZ NACHWEISEN

Banken brauchen ihre Systeme rund um die Uhr. DORA verlangt von ihnen, dass auch ihre Dienstleister Ausfälle übersteht und schnell wieder anläuft. Verfügbarkeit, getestete Wiederanlaufpläne und Business Continuity (Annex A 5.29, 5.30, 8.13) stehen für FinTechs deshalb besonders im Fokus.

PRIVILEGIERTE ZUGÄNGE UND ZAHLUNGSDATEN

Wer an Kernbankensysteme angebunden ist und Zahlungsdaten verarbeitet, verwaltet hochsensible Zugänge. Diese müssen streng vergeben, getrennt und protokolliert werden (Annex A 8.2, 8.3, 8.15). Bei Kartendaten kommt häufig PCI DSS als zusätzliche Anforderung hinzu.

EIGENE DRITTANBIETER UND KONZENTRATION

FinTechs stützen sich selbst auf Cloud- und SaaS-Dienste, über die Finanzdaten laufen. Aufsicht und Kunden achten auf Konzentrationsrisiken und Sub-Dienstleister. Lieferantensteuerung mit Anforderungen und Nachweis (Annex A 5.19 bis 5.23) ist deshalb ein Kernpunkt jeder Prüfung.

BEDROHUNGSLAGE & RISIKEN

Wo FinTechs *konkret angreifbar sind.*

Die Risiken hängen an sensiblen Finanzdaten, an der Anbindung zu Banken und an der hohen Verfügbarkeitserwartung. Fünf Szenarien tauchen in der Praxis immer wieder auf. Sie alle haben eine Gemeinsamkeit: Im Finanzsektor wird aus einem technischen Vorfall schnell ein regulatorisches und ein 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 (Annex A 8.24, 8.2 bis 8.5) sind hier die zentralen und im Audit geprüften Hebel. Hinzu kommen Melde- und Nachweispflichten gegenüber Aufsicht und Kunden, die nur mit lückenloser Protokollierung fristgerecht zu erfüllen sind.

2 · AUSFALL DER OPERATIVEN RESILIENZ

Banken erwarten nahezu durchgehende Verfügbarkeit. Ein längerer Ausfall des FinTechs trifft unmittelbar deren Geschäft und löst unter DORA Melde- und Nachweispflichten aus. Getestete Wiederanlaufpläne und Business Continuity (Annex A 5.29, 5.30, 8.13) entscheiden, wie schnell der Betrieb zurückkehrt. Banken verlangen dafür konkrete Wiederanlaufzeiten und regelmäßige Tests, nicht bloß ein Konzept auf Papier.

3 · GESCHEITERTE BANK-PRÜFUNG

Ein konkretes Geschäftsrisiko. Scheitert der Anbieter an der Auslagerungs- oder DORA-Prüfung eines Instituts, steht der Vertrag auf dem Spiel, oft das Kerngeschäft. Ohne ISO 27001 zieht sich jede Prüfung, und manche endet vorzeitig. Das Zertifikat verschiebt das Gespräch vom Ob zur Umsetzung. Ein vorliegendes Zertifikat verkürzt zudem die Auslagerungsprüfung erheblich, weil das Institut auf einen anerkannten Nachweis zurückgreift.

4 · ANGRIFF ÜBER DIE LIEFERKETTE

FinTechs sind selbst Drittanbieter und stützen sich auf weitere Dienste. Ein kompromittierter Sub-Dienstleister oder ein manipuliertes Update wird zum Einstieg in sensible Umgebungen. Lieferantensteuerung und sichere Entwicklung (Annex A 5.19 bis 5.23, 8.25 bis 8.31) begrenzen dieses Risiko. Aufsicht und Kunden achten dabei besonders auf Konzentrationsrisiken, wenn viele Anbieter auf denselben Cloud-Diensten aufsetzen.

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 (Annex A 8.2, 8.5, 8.15) schließen diese Tür. Gerade bei Fernzugängen externer Dienstleister ist die lückenlose Nachvollziehbarkeit jedes einzelnen Zugriffs entscheidend.

ANFORDERUNGEN DER NORM

Was ISO 27001 *konkret verlangt.*

Die Norm besteht aus zwei Teilen: den Management-Anforderungen in den Kapiteln 4 bis 10, die zertifiziert werden, und dem Annex A mit 93 Sicherheitsmaßnahmen, aus denen risikobasiert ausgewählt wird. Fünf Bausteine bilden den Kern.

KONTEXT UND GELTUNGSBEREICH (KAP. 4)

Am Anfang steht die Frage, was geschützt werden soll. Der Anbieter bestimmt internen und externen Kontext, die Erwartungen wichtiger Parteien wie Banken und Aufsicht und legt den Geltungsbereich des ISMS fest (Kap. 4.3).

Für FinTechs ist der Zuschnitt entscheidend. Der Scope sollte die Plattform und die Dienste abdecken, die Institute tatsächlich prüfen. Ein zu weit gefasster Geltungsbereich ist der häufigste vermeidbare Fehler.

FÜHRUNG UND POLITIK (KAP. 5)

Die Norm macht Sicherheit zur Leitungsaufgabe. Die Geschäftsführung verabschiedet die Informationssicherheitsleitlinie, stellt Ressourcen bereit und weist Rollen zu (Kap. 5.1 bis 5.3). Im stark geprüften Finanzumfeld muss die Spitze das Thema sichtbar und glaubwürdig tragen.

RISIKEN UND SOA (KAP. 6)

Das Herzstück. Der Anbieter legt eine wiederholbare Methode für die Risikoeinschätzung fest, bewertet seine Risiken rund um Finanzdaten, Verfügbarkeit und Zugänge und entscheidet je Risiko über die Behandlung (Kap. 6.1.2 und 6.1.3). Das Ergebnis mündet in die Erklärung zur Anwendbarkeit, die für jede der 93 Maßnahmen begründet, ob sie gilt.

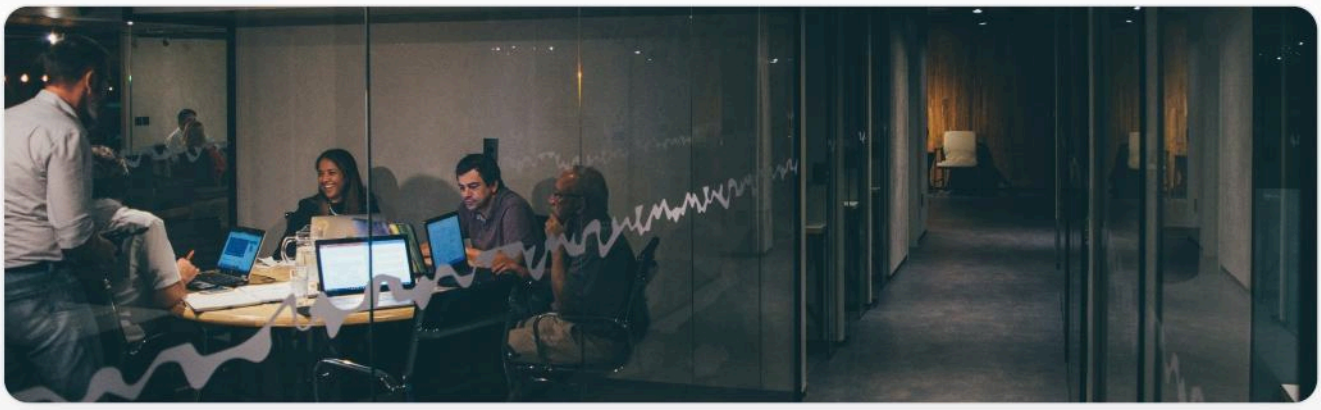
Operative Resilienz, Zugriffskontrolle und Lieferkette stehen für FinTechs fast immer oben auf der Liste.

BETRIEB UND MASSNAHMEN (KAP. 8, ANNEX A)

Die ausgewählten Maßnahmen werden umgesetzt und gelebt. Der Annex A gliedert sie in vier Gruppen: 37 organisatorische, 8 personenbezogene, 14 physische und 34 technische Maßnahmen. Im Finanzumfeld stehen Business Continuity, Zugriffs- und Privileged-Access-Management, sichere Entwicklung und Lieferantensteuerung im Vordergrund.

BEWERTUNG UND VERBESSERUNG (KAP. 9, 10)

Ein ISMS endet nicht mit der Einführung. Internes Audit und Managementbewertung (Kap. 9.2 und 9.3) prüfen regelmäßig die Wirksamkeit, Korrekturmaßnahmen schließen Lücken (Kap. 10.2). Genau diese Schleife will der Auditor sehen, und sie deckt sich mit der laufenden Überwachung, die DORA verlangt.



UMSETZUNG IN DER PRAXIS

In sechs Schritten *zum Zertifikat.*

Der Weg zur Zertifizierung lässt sich planen. Diese Reihenfolge baut aufeinander auf und nutzt die starke Technikbasis von FinTechs, statt bei null zu beginnen. Realistisch sind je nach Reife drei bis sechs Monate bis zum Audit.

Ein ISMS, das einmal steht, trägt ISO 27001, DORA und SOC 2 zugleich. *Ein Fundament, mehrere Nachweise.*

1 · GELTUNGSBEREICH FESTLEGEN

Kontext klären und den Scope auf die Plattform und die Dienste schneiden, die Institute prüfen. Ein klarer Geltungsbereich ist die Grundlage für alles Weitere und der wirksamste Hebel, um den Aufwand niedrig zu halten.

2 · FÜHRUNG UND LEITLINIE

Die Geschäftsführung verabschiedet die Sicherheitsleitlinie, benennt eine verantwortliche Person und stellt Ressourcen bereit. In technikgetriebenen FinTech-Teams ist dieser Schritt schnell erledigt, wenn die Spitze dahintersteht.

3 · RISIKEN ANALYSIEREN

Assets erfassen, von der Plattform über Bank-Anbindungen bis zu den genutzten Cloud- und SaaS-Diensten. Risiken bewerten, Verfügbarkeit und Datenschutz besonders gewichten und die Erklärung zur Anwendbarkeit erstellen. Eine gute Analyse macht den Aufwand planbar.

4 · MASSNAHMEN UMSETZEN

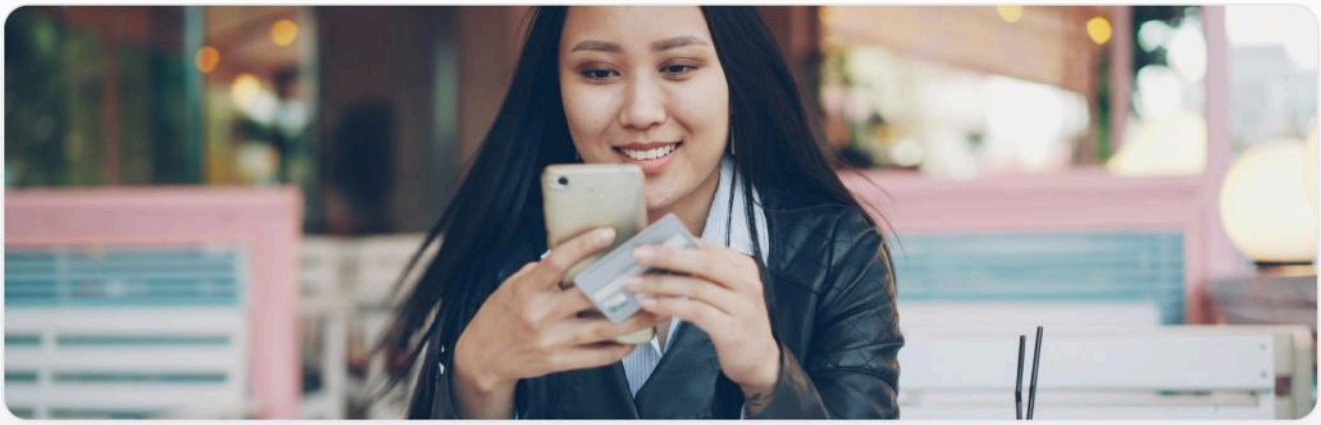
Die ausgewählten Annex-A-Maßnahmen einführen und dokumentieren. Mit den wirksamsten Hebeln beginnen: Business Continuity, Zugriffs- und Privileged-Access-Management, sichere Entwicklung und Lieferantenanforderungen. Wo möglich, Nachweise automatisieren.

5 · INTERN AUDITIEREN UND BEWERTEN

Vor dem Zertifizierungsaudit prüft ein internes Audit die Wirksamkeit, die Managementbewertung zieht Bilanz. Diese Schleife einmal vollständig zu durchlaufen ist Pflicht und zugleich die beste Generalprobe, auch für künftige Bank-Audits.

6 · ZERTIFIZIERUNGSAUDIT BESTEHEN

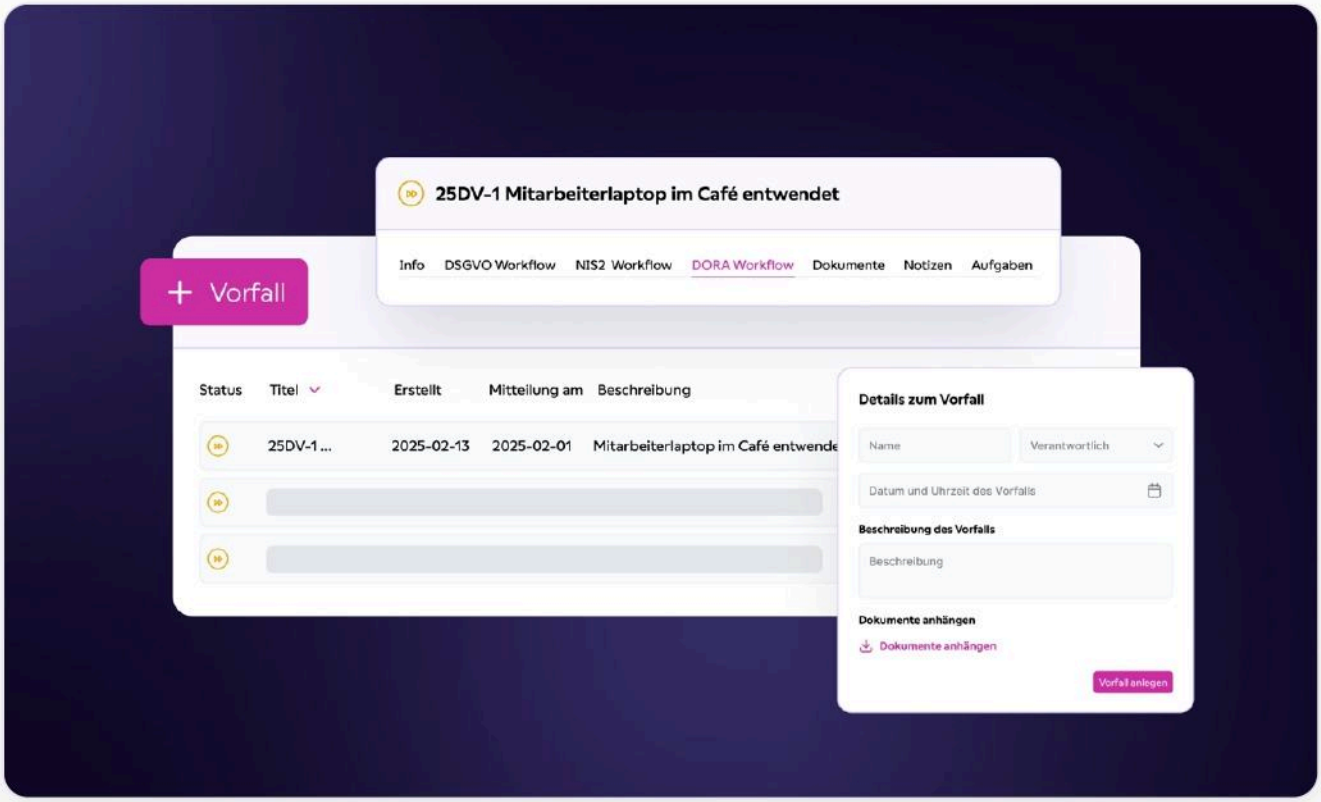
Das externe Audit läuft in zwei Stufen: Dokumentenprüfung (Stage 1) und Wirksamkeitsprüfung (Stage 2). Danach folgt das Zertifikat, gültig für drei Jahre mit jährlichen Überwachungsaudits. Wer DORA-Nachweise oder SOC 2 ergänzt, baut auf demselben Fundament auf.



WIE SECJUR ES EINFACH MACHT

Von der Bank-Anforderung zur *auditbereiten Umsetzung.*

Das Digital Compliance Office (DCO) führt FinTech-Anbieter durch die gesamte ISO-27001-Umsetzung: Geltungsbereich, Risikoanalyse, operative Resilienz, Lieferantensteuerung und Nachweise an einem Ort, mehrere Frameworks parallel. Statt monatelanger Beratung und einem Dutzend Tabellen 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.



Risiko & Resilienz

Geführte Risikoanalyse und ein strukturierter Umgang mit Vorfällen und Wiederanlauf, genau die operative Resilienz, die DORA und die Banken verlangen.

Lieferanten & Audit-Rechte

Lieferantensteuerung und revisionssichere Nachweise, mit denen Sie Auslagerungs- und DORA-Klauseln samt Audit-Rechten verlässlich bedienen.

Mehrere Frameworks

ISO 27001, DORA-Nachweise und SOC 2 laufen auf einem gemeinsamen ISMS, gemeinsame Maßnahmen werden nur einmal gepflegt statt dreimal.

SO LÄUFT DIE EINFÜHRUNG

Der Einstieg ist schlank. Sie legen den Geltungsbereich fest, das DCO führt Sie durch jede Anforderung, und wo eine Expertin nötig ist, ist sie zugeschaltet. Sie entscheiden, das System dokumentiert im Hintergrund. So wird aus vorhandener Technik in Wochen ein auditbereites ISMS, das auch Bank-Prüfungen standhält.

EIN FUNDAMENT, MEHRERE NACHWEISE

Weil sich ISO 27001, DORA 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 bei schnellen Releases aktuell bleibt.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen *arbeiten mit SECJUR.*

FinTechs, Zahlungsdienstleister, Software-Häuser und digitale Dienstleister erfüllen mit dem DCO ihre Sicherheitsanforderungen 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

reanmo

REFERENZEN AUS FINTECH, FINANCIAL SOFTWARE UND PAYMENTS

vestlane · NYALA · AEQUITA · BILTON · Tomorrow · EDEKABANK

AUDIT-ERFOLG
100%
Erfolgsquote in bisherigen Zertifizierungsaudits.

SCHNELLER
50%
Weniger Aufwand gegenüber klassischer Beratung.

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

STANDARDS
10+
Frameworks parallel abgedeckt, ohne Doppelarbeit.

WARUM FINTECHS SECJUR WÄHLEN

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

Der digitale Compliance-Officer (DCO) bündelt Richtlinien, Aufgaben und Nachweise an einem Ort und verteilt Verantwortlichkeiten automatisch an die richtigen Personen. Über 60 Integrationen holen Belege direkt aus den Systemen, sodass das ISMS aktuell bleibt, ohne dass jemand Tabellen pflegt.

Weil derselbe Unterbau ISO 27001, DORA und SOC 2 zugleich trägt, ist die regulatorische Pflicht mit einem Aufbau erfüllt, statt in getrennten Projekten abgearbeitet zu werden.

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur das Zertifikat an der Wand, 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.

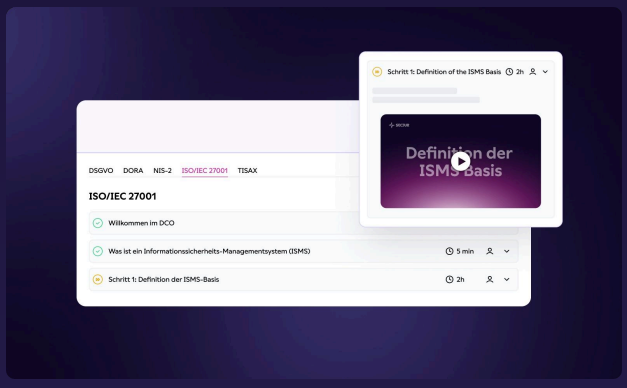
So wird aus einer Pflicht ein dauerhafter Wettbewerbsvorteil, der den Zugang zu Banken und Enterprise-Kunden sichert und die nächste Finanzierungsrunde stützt.

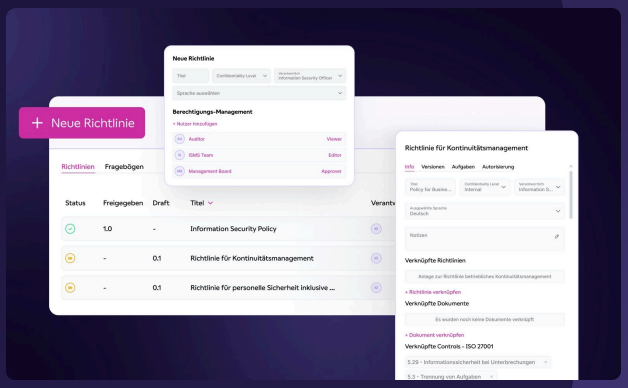
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR

Masterplan.com · 1KOMMA5° · yfood · deepset · Tomorrow · AllDent Zahnzentrum

www.secjur.com