Digital Operational Resilience Act

DORA leicht gemacht: Ihre Roadmap zur digitalen Resilienz im Finanzsektor

Erfahren Sie, wie Banken für digitale Resilienz ihrer Geschäftsprozesse sorgen, und wie die Aufrüstung zu DORA-konformen Prozessen ihr Unternehmen weiterbringt.

So machen Sie Ihre Bank fit für DORA

Februar 2025

Inhalt

01. Einführung: Warum Resilienz unverzichtbar ist und **wie DORA die Spielregeln ändert**

1.1. Warum digitale Resilienz im Finanzsektor so wichtig ist

Die digitale Transformation hat den Finanzsektor grundlegend verändert. Während diese Technologien neue Geschäftsmöglichkeiten eröffnen, steigt gleichzeitig die Verwundbarkeit gegenüber Cyberbedrohungen deutlich an. Finanzdienstleister sind hier besonders anfällig. Ob Zahlungsverkehr, Wertpapierhandel oder Kundenservice: Nahezu alle wesentlichen Geschäftsprozesse basieren heute auf vernetzten IT-Systemen. Ein erfolgreicher Cyberangriff kann daher weitreichende Folgen haben. Sie reichen von Datenlecks über Systemausfälle bis hin zu massiven Reputationsschäden.

Aktuelle Zahlen belegen die Brisanz: In der Schweiz ist die Anzahl der Meldungen beim Bundesamt für Cybersicherheit von 10'833 im Jahr 2020 auf inzwischen 49'380 hochgeschnellt. In Deutschland stellt das Bundesamt für Sicherheit in der Informationstechnik kurz und knapp fest: «Die Lage der IT-Sicherheit in Deutschland war und ist besorgniserregend.» Die Schäden durch Datendiebstahl, Industriespionage oder Sabotage in Deutschland beliefen sich im Jahr 2024 auf über 266 Milliarden Euro.

1.2. Hintergründe der DORA-Verordnung

Als Reaktion auf diese Herausforderungen hat die Europäische Union den Digital Operational Resilience Act (DORA) ins Leben gerufen. Die Verordnung schafft erstmals einen einheitlichen europäischen Rahmen für die «digitale Widerstandsfähigkeit» im Finanzsektor.

Anders als bisherige nationale Regelungen verfolgt DORA einen ganzheitlichen Ansatz: Neben technischen Sicherheitsanforderungen reguliert sie ebenso organisatorische Aspekte wie Risikomanagement, Incident Response und die Überwachung von IT-Dienstleistern. Das alles soll letztlich dafür sorgen, dass sich Finanzinstitute und ihre Servicepartner proaktiv auf mögliche Krisen und Vorfälle vorbereiten.
Besonders weitreichend sind die neuen Vorgaben an das Management von Drittanbieterrisiken – ein Bereich, der angesichts zunehmender IT-Auslagerungen immer wichtiger wird.

INFOBOX

Was bedeutet «Resilienz»?

Der Begriff der Resilienz stammt ursprünglich aus der Psychologie und beschreibt die Fähigkeit, Krisen zu bewältigen und als Anlass für positive Entwicklungen zu nutzen. Im IT-Kontext bezeichnet «digitale Resilienz» die Fähigkeit einer Organisation,

- Cyberangriffe und digitale Störungen abzuwehren,
- bei erfolgreichen Angriffen den Schaden zu begrenzen,
- zentrale Geschäftsprozesse auch während eines Vorfalls aufrechtzuerhalten und
- den Betrieb nach Störungen schnell wieder aufzunehmen und aus Vorfällen zu lernen.

§ Eine offizielle Definition für «digitale operationale Resilienz» findet sich in Artikel 3 des Rechtsakts.

02. **DORA in Kürze:** Was Finanzinstitute wissen müssen

Das DORA-Regelwerk verfolgt drei Hauptziele. Erstens will sie die digitale Betriebsfähigkeit von Finanzunternehmen stärken. Zweitens harmonisiert sie die Standards zur Cyber Security in der EU. Und drittens schafft sie einen einheitlichen Aufsichtsrahmen für IT-Dienstleister im Finanzsektor.

DORA gilt dabei für nahezu alle regulierten Finanzinstitute in der EU, darunter:

- Banken und Kreditinstitute
- Versicherungsgesellschaften
- Wertpapierfirmen und Börsen
- Zahlungsdienstleister und E-Geld-Institute
- Fondsgesellschaften und Vermögensverwalter

§ Eine offizielle Auflistung aller betroffenen Unternehmen findet sich in Artikel 2 der Verordnung. Mehr Informationen zu den zuständigen Behörden sind in Artikel 46 festgehalten.

Wichtig: Auch IT-Anbieter, die essentielle Services für diese Unternehmen erbringen, fallen unter die DORA-Regulierung, selbst wenn sie ihren Sitz ausserhalb der EU haben.
Das Regelwerk ist bereits am 17. Januar 2023 in Kraft getreten, mit einer Übergangsfrist von zwei Jahren zur Implementierung. Ab 17. Januar 2025 müssen sich betroffene Anbieter also an alle Vorgaben halten.

INFOBOX

Verordnung vs. Richtlinie
Anders als eine EU-Richtlinie gilt die DORA-Verordnung unmittelbar in allen EU-Mitgliedstaaten. Sie muss also nicht erst in nationales Recht umgesetzt werden. Auch Schweizer Finanzdienstleister sind sofort betroffen, wenn sie Geschäfte in der EU tätigen oder IT-Dienstleistungen für EU-Finanzinstitute erbringen.

03. Regulatorische Schwerpunkte: **Die wichtigsten Handlungsfelder im Überblick**

DORA definiert sechs zentrale Handlungsfelder, in denen Unternehmen im Finanzbereich Massnahmen ergreifen müssen:

1. **IKT-Risikomanagement:** Aufbau eines umfassenden Rahmenwerks, um IT-Risiken zu identifizieren, zu bewerten und mit ihnen umzugehen.
2. **Vorfallmanagement:** Standardisierte Prozesse, um IT-Vorfälle zu erkennen, klassifizieren und melden.
3. **Digitale Resilienz-Tests:** Die Widerstandsfähigkeit ist durch verschiedene Testverfahren regelmässig zu überprüfen.
4. **Management von Drittanbieterrisiken:** Strenge Vorgaben für Auswahl, Überwachung und Kontrolle von IT-Servicepartnern.
5. **Überwachung kritischer Anbieter:** Spezielle Vorschriften für die Zusammenarbeit mit systemrelevanten IT-Anbietern.
6. **Informationsaustausch:** Teilnahme an Threat Intelligence Sharing und Krisenübungen.

Diese sechs Bereiche bilden das Fundament der DORA-Vorschriften. Folgend betrachten wir sie im Detail und zeigen auf, welche konkreten Schritte sich daraus ergeben.

3.1. IKT-Risikomanagement

DORA verpflichtet Intitute der Finanzbranche, ein umfassendes Rahmenwerk für ihr IKT-Risikomanagement zu etablieren. Im Zentrum steht dabei, Risiken gezielt zu identifizieren, bewerten, überwachen und verringern.

§

«Finanzunternehmen verfügen über einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen, der Teil ihres Gesamtrisikomanagementsystems ist und es ihnen ermöglicht, IKT-Risiken schnell, effizient und umfassend anzugehen und ein hohes Niveau an digitaler operationaler Resilienz zu gewährleisten.» – Artikel 6, Absatz 1

Das Regelwerk fordert explizit, dass die Geschäftsleitung aktiv in die Steuerung eingebunden sein muss. Sie trägt die Gesamtverantwortung für die Umsetzung des Rahmenwerks. Dazu gehört auch, dass klare Rollen und Verantwortlichkeiten für das Risikomanagement definiert werden müssen.

§

«Das Leitungsorgan des Finanzunternehmens definiert, genehmigt, überwacht und verantwortet die Umsetzung aller Vorkehrungen im Zusammenhang mit dem IKT-Risiko-managementrahmen nach Artikel 6 Absatz 1.» – Artikel 5, Absatz 2

Ein weiterer zentraler Punkt: Betroffene Unternehmen müssen ihre IT-Systeme und -Prozesse vollständig dokumentieren. Dies bildet die Grundlage für regelmässige Überprüfungen und Aktualisierungen des Rahmenwerks, die DORA ebenfalls vorschreibt.

PRAXIS TIPPS

Empfehlungen
Wir empfehlen, beim Aufbau des IKT-Risikomanagements nach DORA diese bewährten Prinzipien zu beachten:

- Bestehende Risikomanagement-Prozesse als Basis nutzen
- Interdisziplinäres Team für die Umsetzung zusammenstellen
- Externe Expertise bei Bedarf frühzeitig einbinden
- Zeit für Tests und Anpassungen einplanen.

Checkliste
✓ Rahmenwerk zur Steuerung von IKT-Risiken implementieren
✓ Geschäftsleitung aktiv einbinden
✓ Rollen und Verantwortlichkeiten festlegen
✓ IT-Systeme und -Prozesse dokumentieren
✓ Regelmässige Überprüfungen einplanen und umsetzen

3.2. IKT-Vorfälle melden und klassifizieren

DORA führt EU-weit einheitliche Standards dazu ein, wie Finanzdienstleister mit IT-Sicherheitsvorfällen umgehen. Der Rechtsakt legt hier präzise fest, welche Vorfälle zu melden sind und wie Unternehmen dabei vorgehen müssen.

Als «schwerwiegend» stuft DORA dabei IT-Vorfälle ein, die den normalen Betrieb erheblich stören oder zu bedeutenden finanziellen Verlusten führen können. Solche Vorfälle müssen Unternehmen unverzüglich an die zuständige Aufsichtsbehörde melden, auch wenn noch nicht alle Details des Vorfalls bekannt sind.

Die Meldung «erheblicher Cyberbedrohungen» ist hingegen freiwillig. Dies meint Probleme oder Entwicklungen, die künftig zu einem Betriebs- oder Sicherheitsvorfall führen könnten.

§ Mehr Informationen zu den Meldepflichten finden sich in Artikel 19.

PRAXIS TIPPS

Empfehlungen

Um im Ernstfall schnell und richtig reagieren zu können, sollten Sie:

- Klare Prozesse für die Erkennung und Klassifizierung von Vorfällen definieren
- Vorlagen für Meldungen an die Aufsicht vorbereiten
- Regelmässig Notfallübungen einplanen
- Ein Krisenkommunikationsteam zusammenstellen

Checkliste

✓ Prozess zur Erkennung schwerwiegender IT-Vorfälle einrichten
✓ Meldewege an Aufsichtsbehörden etablieren
✓ System zur Dokumentation aller IT-Vorfälle aufbauen
✓ Erhebliche Cyberbedrohungen melden
✓ Vorfälle fundiert analysieren

3.3. Digitale Resilienz-Tests

DORA verpflichtet die betreffenden Unternehmen, ihre technische Infrastruktur regelmässig zu testen. Diese Tests sollen feststellen, wie widerstandsfähig die Systeme gegen verschiedene Arten von Störungen und Angriffen sind.

Das Regelwerk unterscheidet dabei verschiedene Testarten: Neben grundlegenden technischen Tests wie Schwachstellenscans müssen Unternehmen auch komplexere Überprüfungen einplanen. Besonders wichtig sind die sogenannten «Threat Led Penetration Tests» (TLPT): Sie simulieren realistische Angriffsszenarien. Die Tests werden dabei von «unabhängigen, internen oder externen Parteien» umgesetzt (Artikel 24, Absatz 4).

Wie oft Unternehmen solche Tests einplanen müssen, hängt von ihrer Grösse und Bedeutung für das Finanzsystem ab. DORA schreibt vor, dass die Testergebnisse zu dokumentieren und dem Management vorzulegen sind. Entdeckte Schwachstellen sind zeitnah zu beheben.

§ Mehr Informationen dazu sind in Kapitel IV der Verordung zu finden.

PRAXIS TIPPS

Empfehlungen

Für effektive Tests empfehlen wir:

- Realistische Szenarien, die typische Bedrohungen abbilden
- Verschiedene Unternehmensbereiche in Tests einbinden
- Ergebnisse zielgerichtet auswerten und Massnahmen ableiten
- Tests als kontinuierlichen Prozess verstehen

Checkliste

✓ Regelmässige Tests der Informationssysteme einplanen und umsetzen
✓ Unabhängige Experten für TLPT beauftragen
✓ Testergebnisse dokumentieren
✓ Management informieren
✓ Schwachstellen beheben

3.4. Management von IKT-Drittparteienrisiken

DORA widmet gerade auch dem Umgang mit Service-Providern besondere Aufmerksamkeit. Die Vorschrift reagiert damit auf die zunehmende Auslagerung wesentlicher IT-Funktionen.
Akteure der Finanzbranche müssen deshalb nun alle ihre IT-Dienstleister in einem zentralen Register erfassen. DORA verlangt dabei, dass sie die Risiken jeder Auslagerung exakt bewerten. Besonders wichtig: Unternehmen müssen klar dokumentieren, welche ihrer ausgelagerten Funktionen sie als «kritisch» oder «wichtig» einstufen.
Darüber hinaus gelten neue Standards für Verträge mit diesen Servicepartnern: Diese müssen detailliert regeln, wie der Anbieter die Sicherheit und Verfügbarkeit seiner Services gewährleistet. Zudem schreibt DORA vor, dass Finanzdienstleister Exit-Strategien entwickeln, um im Notfall schnell zu einem anderen Anbieter zu wechseln.

§ Mehr Informationen zu diesem Thema finden sich in Kapitel V der Verordnung.

PRAXIS TIPPS

Empfehlungen
Um die DORA-Bestimmungen effizient umzusetzen, sollten Sie:

- Bestehende Verträge überprüfen
- Standardisierte Bewertungskriterien für Service-Provider entwickeln
- Regelmässige Kontrollen der Dienstleisterqualität einplanen
- Alternative Anbieter für zentrale Services identifizieren

Checkliste
✓ Register aller IT-Anbieter erstellen
✓ Kritische Funktionen identifizieren
✓ Verträge DORA-konform gestalten
✓ Risiken systematisch bewerten
✓ Exit-Strategien entwickeln

3.5. Überwachung kritischer IKT-Drittdienstleister

DORA führt erstmals eine direkte Aufsicht jener IT-Servicepartner ein, die für den Finanzsektor besonders wichtig sind. Die EU-Aufsichtsbehörden stufen solche Anbieter als «kritische IKT-Drittdienstleister» ein und unterwerfen sie einem speziellen Überwachungsrahmen.
Sie müssen etwa nachweisen, dass sie die DORA-Vorschriften erfüllen – unabhängig davon, ob sie ihren Sitz in der EU haben oder nicht. Die Aufsicht kann Vor-Ort-Prüfungen durchführen und bei Mängeln Massnahmen anordnen.
Für Finanzinstitute bedeutet dies: Sie müssen prüfen, ob ihre externen Partner so eingestuft sind. In diesem Fall müssen sie sicherstellen, dass ihre Verträge die erforderlichen Prüfungs- und Kontrollrechte der Aufsicht berücksichtigen.

§ Weitere Informationen zur Einstufung finden sich in Artikel 31, Absatz 2.

PRAXIS TIPPS

Empfehlungen
Wir empfehlen:

- Mit wichtigen IT-Dienstleistern über DORA zu sprechen:
  - Werden sie als kritische Anbieter eingestuft?
  - Entsprechen deren Compliance-Prozesse den DORA-Anforderungen?
  - Werden Sicherheitsmassnahmen dokumentiert?
- Entsprechende Vertragsanpassungen umzusetzen
- Alternativlösungen für essentielle Services entwickeln

Checkliste
✓ Kritische IT-Anbieter identifizieren
✓ Aufsichtsrechte in Verträgen verankern
✓ Kontrollprozesse implementieren
✓ Zusammenarbeit mit Aufsicht sicherstellen
✓ Notfallpläne erstellen

3.6. Informationsaustausch und Krisenübungen

Um den Finanzsektor besser auf IT-Krisen vorbereiten, sieht das Regelwerk zwei wichtige Instrumente vor: den strukturierten Austausch von Bedrohungsinformationen und gemeinsame Krisenübungen.
Institute der Finanzbranche können deshalb Vereinbarungen treffen, um Informationen über Cyberbedrohungen und Schwachstellen auszutauschen. DORA schafft dafür einen rechtlichen Rahmen und legt fest, wie dieser Austausch datenschutzkonform zu gestalten ist (siehe dazu Artikel 45 der Verordnung). So sollen die Unternehmen voneinander lernen und sich gegenseitig vor aktuellen Bedrohungen warnen.
DORA verpflichtet zudem grössere Finanzinstitute, an sektorweiten Krisenübungen teilzunehmen. Diese Übungen sollen realistische Szenarien simulieren wie etwa grossflächige Cyberangriffe oder den Ausfall wichtiger IT-Drittanbieter. Die Unternehmen müssen im Zuge dessen nachweisen, dass sie auch in Krisensituationen handlungsfähig bleiben.

§ Mehr Informationen dazu finden sich in Artikel 49.

PRAXIS TIPPS

Empfehlungen
Um den maximalen Nutzen aus den Übungen zu ziehen, sollten Sie:

- Interne Krisenprozesse vorab testen
- Alle relevanten Bereiche einbinden
- Erkenntnisse dokumentieren
- Schwachstellen konsequent beheben

Checkliste
✓ Prozesse für Informationsaustausch etablieren
✓ Datenschutzkonforme Sharing-Vereinbarungen treffen
✓ An Krisenübungen teilnehmen
✓ Krisenmanagement regelmässig testen
✓ Erkenntnisse in Massnahmen umsetzen

04. Mit DSwiss zur digitalen Resilienz: **Lösungen für DORA-Compliance**

SecureExchange ist eine leistungsfähige Lösung für den papierlosen Austausch sensibler Daten. Die Plattform zentralisiert und vereinfacht das Dokumentenmanagement mit Kunden und gewährleistet dabei die Einhaltung von Datenschutzvorschriften.
Statt Dokumente über verschiedene Kanäle wie E-Mail, Post oder persönliche Meetings auszutauschen, läuft die gesamte Kommunikation über einen zentralen, hochsicheren Kanal. Dieser ist sowohl über Desktop-Computer als auch mobile Geräte zugänglich.

4.1. SecureExchange

DORA verpflichtet Intitute der Finanzbranche, ein umfassendes Rahmenwerk für ihr IKT-Risikomanagement zu etablieren. Im Zentrum steht dabei, Risiken gezielt zu identifizieren, bewerten, überwachen und verringern.

Besondere Merkmale auf einen Blick:

- Vertraulicher, direkter Austausch von Dateien bis zu 2 GB
- Unterstützung verschiedener Dokumentenformate
- Einfacher Zugang über sichere E-Mail-Links – keine Software-Installation oder Kontoerstellung für Empfänger nötig
- Dediziertes Portal für Provider und Administratoren zur Benutzerverwaltung
- Flexible Stellvertretungsregelung für Kundenfälle
- Zentrales Interface für Kundenberater mit anpassbarer Ordnerstruktur

Vorteile mit Blick auf DORA:

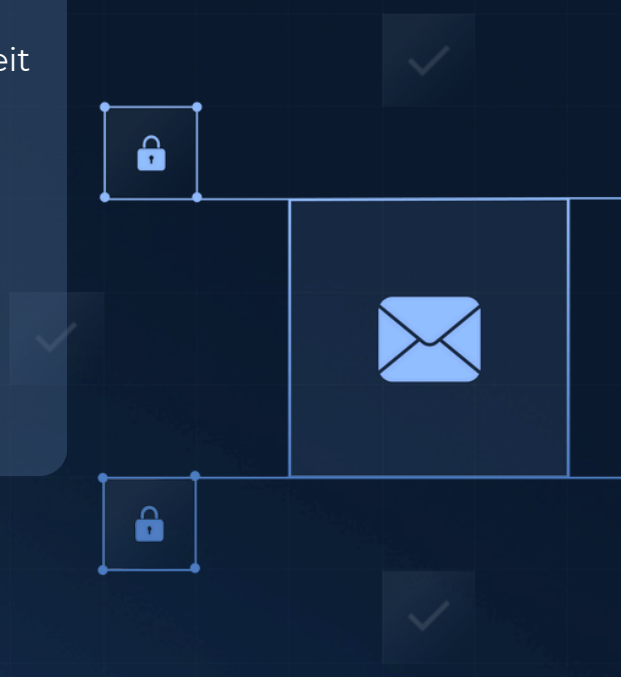
- Unterstützt das IKT-Risikomanagement durch zentralisierten, kontrollierten Dokumentenaustausch statt verschiedener unsicherer Kanäle
- Hilft bei der Dokumentation durch zentrale Verwaltung aller Austauschprozesse
- Vereinfacht das Management von Zugriffsrechten durch das Admin-Portal
- Ermöglicht Business Continuity durch Stellvertretungsregelungen

4.2. Postbox

Postbox ist eine vertrauenswürdige und rechtskonforme Lösung für die papierlose Übermittlung und dauerhafte Speicherung von Dokumenten. Sie lässt sich direkt in bestehende Systeme integrieren.
Postbox speichert versandte Dokumente permanent und unveränderbar. Diese gehen dabei direkt in das Eigentum der Empfänger über. Die Lösung erfüllt damit die Kriterien eines dauerhaften Datenträgers gemäss den Vorgaben des Europäischen Gerichtshofs (EuGH).

Besondere Merkmale auf einen Blick:

- Dezentrale Lösung für erhöhte Zuverlässigkeit
- Ende-zu-Ende-Verschlüsselung während Übertragung und Speicherung
- Skalierbar für Millionen von Dokumenten ohne Leistungseinbussen
- Reduziert Papierverbrauch und Betriebskosten
- Erfüllt alle rechtlichen Auflagen für dauerhafte Datenspeicherung



Vorteile mit Blick auf DORA:

- Stärkt die digitale Resilienz durch dezentrale Architektur
- Bietet Nachweisbarkeit durch unveränderbare Speicherung
- Unterstützt Incident Response durch Ende-zu-Ende-Verschlüsselung und abgesicherte Speicherung
- Reduziert operationelle Risiken durch Integration in bestehende Systeme

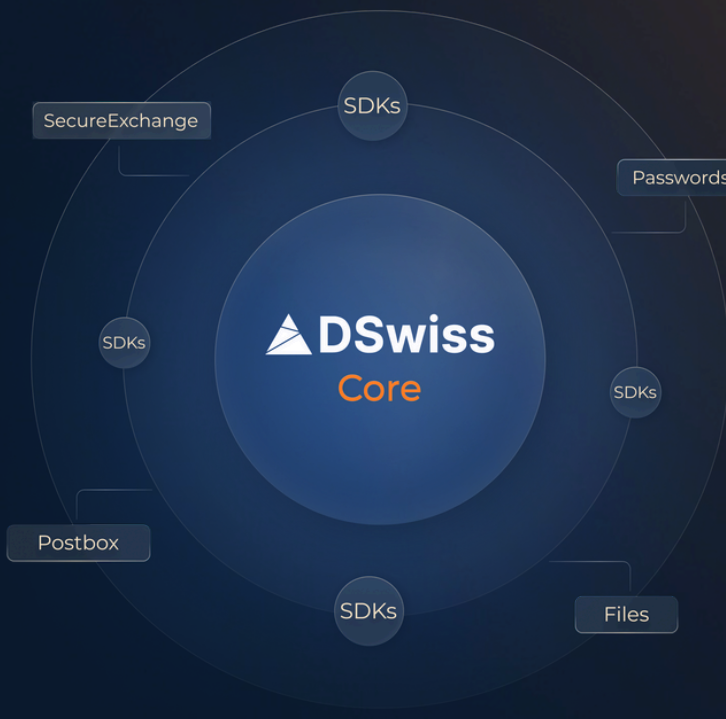
4.3. SecureData Platform

Die SecureData Platform ermöglicht es Kunden, eine massgeschneiderte Datensicherheitslösung aufzubauen. Sie kombiniert verschiedene Module für Passwort- und Dateiverwaltung, Datenaustausch und Dokumentenübermittlung – jeweils optimal auf den spezifischen Anwendungsfall zugeschnitten.

Die Plattform basiert auf der langjährigen Erfahrung von DSwiss in der Entwicklung von Datensicherheitssoftware. Sie bietet Kunden die Flexibilität, neue Module zu integrieren, wenn sich ihr Geschäft weiterentwickelt. Dabei wächst die Lösung nahtlos mit und gewährleistet stets die Einhaltung von Datenschutzstandards.

Besondere Merkmale auf einen Blick:

- Modularer Aufbau für maximale Flexibilität
- Bewährte Technologie
- Einfache Integration neuer Module
- Skalierbare Architektur
- Compliance mit Datenschutzvorgaben



Vorteile mit Blick auf DORA:

- Ermöglicht modularen Aufbau der IT-Sicherheit
- Wächst mit steigenden regulatorischen Auflagen
- Unterstützt verschiedene Aspekte des IKT-Risikomanagements durch kombinierbare Module
- Bietet Flexibilität bei der Implementierung neuer Sicherheitsanforderungen

05. Von regulatorischer Vorgabe zur strategischen Change: **DORA als Wegbereiter für Innovation**

DORA bedeutet für viele Finanzunternehmen zunächst zusätzlichen Aufwand. Doch wer die neuen Regelungen konsequent umsetzt, stärkt damit nachhaltig seine digitale Resilienz. In einer Zeit, in der Cyberbedrohungen stetig zunehmen, ist dies ein entscheidender Wettbewerbsvorteil.

Dieses Regelwerk schafft dabei erstmals einheitliche Standards für den gesamten europäischen Finanzsektor. Dies vereinfacht die grenzüberschreitende Zusammenarbeit und schafft Rechtssicherheit – gerade auch für Schweizer Unternehmen, die mit EU-Partnern kooperieren.

Die Verordnung ist so gesehen mehr als nur eine weitere regulatorische Vorgabe. Sie bietet die Gelegenheit, bestehende IT-Strukturen zu optimieren und sich für die digitalen Herausforderungen der Zukunft optimal aufzustellen.

Starten Sie Ihre digitale Transformation mit DSwiss

Unverbindlich kontaktieren