DORA in der Assekuranz:
Schlanke Umsetzung, klare Prioritäten

Viele IDV-Tools erfüllen DORA (noch) nicht – droht die nächste Prüfungspanne?

Mit dem **Digital Operational Resilience Act (DORA)** der EU ist seit dem 17. Januar 2025 eine neue regulatorische Ära für Banken, Versicherungen und Finanzdienstleister angebrochen. Ziel ist ein einheitlicher, europaweiter Rahmen für die **digitale operationale Resilienz**, also die Fähigkeit, trotz Cyberangriffen, Systemausfällen oder Drittparteiausfällen funktionsfähig zu bleiben.

Für deutsche Versicherer bedeutet DORA nicht nur eine Verschärfung bestehender IT-Anforderungen, sondern auch das faktische **Auslaufen der VAIT** (Versicherungsaufsichtliche Anforderungen an die IT), die durch die BaFin mit Blick auf Solvency II etabliert wurden. Mit DORA rückt nun ein unmittelbar geltendes EU-Recht in den Mittelpunkt, das nicht nur IT-Abteilungen, sondern das gesamte Unternehmen betrifft, und damit insb. **das Risikomanagement sowie das Aktuariat**. Entscheidend für eine nachhaltige DORA-Umsetzung ist ein **holistischer Risikomanagement-Ansatz**, der alle relevanten Bereiche einbindet und das verbreitete **Silo-Denken aufbricht**.

Der Übergang zur europäischen Regulierung erfolgt nicht automatisch, er verlangt aktives Handeln. Auch für Unternehmen, die noch nicht weit in der Umsetzung sind, bietet sich jetzt die Chance: **zügig nachziehen und regulatorisch wie operativ Sicherheit gewinnen.**

Von der VAIT zu DORA: Was ist neu?

DORA baut auf bestehenden Standards wie VAIT, MaRisk (Mindestanforderungen an das Risikomanagement) und den EIOPA IKT-Guidelines (Informations- und Kommunikationstechnologien) auf, **geht aber weit darüber hinaus**. Die Anforderungen an

- das **IKT-Risikomanagement**,
- die **Behandlung, Klassifizierung und Berichterstattung von IKT-Vorfällen**,
- das **Management von IKT-Drittparteirisiken**,
- sowie das **Testen der digitalen operationalen Resilienz**

werden nicht nur präzisiert, sondern auch erstmals **verbindlich und harmonisiert auf EU-Ebene geregelt**.

> Entscheidend: DORA zielt nicht nur auf klassische IT-Systeme, sondern auf **alle IKT-Dienste**, inklusive Schatten-IT und dezentraler Eigenentwicklungen, insb. auch **IDV-Anwendungen** (Individuelle Datenverarbeitung), wie sie etwa im Risikomanagement und Aktuariat häufig vorkommen.

Cominia Aktuarielle Services GmbH
Geschäftsführer
Dr. Maximilian Happacher,
Dr. Björn Medeke, Sven Müller

Sitz: Hamburg
Handelsregister: Amtsgericht Hamburg
HRB 178526, USt-ID DE357961663

Hausanschrift Hamburg
Cominia Aktuarielle Services GmbH
Überseering 32
22297 Hamburg

Hausanschrift Düsseldorf
Cominia Aktuarielle Services GmbH
Rather Straße 110a
40476 Düsseldorf

Gap-Analyse als pragmatischer Einstieg

Viele Versicherungsunternehmen verfügen bereits über dokumentierte IT-Prozesse im Rahmen von Solvency II und VAIT, auch im Kontext IDV. Dennoch empfiehlt es sich zum Einstieg in die DORA-Umsetzung, eine gezielte **Gap-Analyse im Abgleich mit den zentralen DORA-Anforderungen** durchzuführen, um bestehende Schwachstellen frühzeitig zu erkennen und gezielt priorisierte Maßnahmen abzuleiten. Diese sollte insbesondere folgende Aspekte erfassen:

- Methodik zur **Identifikation kritisch-wichtiger Prozesse und IKT-Dienste**
- Aufbau eines **vom Vorstand verabschiedeten IKT-Risikomanagements** inkl. des IKT-Risikomanagementrahmens
- **Dokumentation** von **Auslagerungen und Drittparteien insb. das Informationsregister**
- **Business-Continuity-Management-Komponenten** wie Notfallplanung und Wiederanlauftests
- **Meldeprozesse** für **schwerwiegende IKT-Vorfälle** (intern und extern)

> Für Risikomanagement, Aktuariate und IT gilt jetzt: **frühzeitig Lücken identifizieren, Governance nachholen, Risiken einschätzen und Dokumentation aufbauen**. Die Zeit für strategische Positionierung ist **jetzt**.

IDV im Einsatz: Weitergehende Pflichten, schärfere Kontrollen

Besonders hoher **Handlungsdruck** besteht im **Risikomanagement und den Aktuariaten**: Die dort genutzten IDV-Anwendungen, etwa Excel-Tools, Access-Datenbanken oder selbst entwickelte Skripte, sind oft **kritisch für die Rückstellungsberechnung, Solvency II, Tarifierung und die regulatorische Finanzberichterstattung**. Obwohl Risikomanagement-Strukturen grundsätzlich etabliert sind, zeigt die Praxis immer wieder, dass viele IDV-Anwendungen noch nicht in ein formalisiertes Risikomanagement eingebunden sind. Hier bietet sich die **Chance**, bestehende **Lücken bei Dokumentation, Testing und Revisionssicherheit** gezielt zu **schließen** und so die Resilienz nachhaltig zu stärken.

Der *RTS Risk Management (Art. 16 (9))* unter DORA hebt die bisherige **Sonderbehandlung IDV** im Rahmen der VAIT auf und stellt selbst entwickelte **IDV-Anwendungen und** zugekaufte **Standardsoftware regulatorisch gleich**.

> Damit unterliegen alle außerhalb der IT-Funktion entstandenen **(IDV)-Anwendungen**, auch solche aus den Fachbereichen, **denselben strengen Prüf- und Dokumentationspflichten** wie zentrale IT-Systeme.

DORA bringt damit erstmals verbindliche, umfassende Anforderungen für den sicheren Einsatz von IDV, die weit über VAIT hinausgehen: Sämtliche IDV-Lösungen sind lückenlos zu **inventarisieren, zu dokumentieren und einem vollständigen Lebenszyklus-management** zu unterwerfen. Dazu gehören verpflichtende Quellcode-Prüfungen, regelmäßiges Schwachstellenmanagement, konsequente Maßnahmen-verfolgung sowie der grundsätzliche Verzicht auf Produktionsdaten in Test- und Entwicklungsumgebungen. Auch Dritt- und Open-Source-Komponenten müssen vor dem Einsatz geprüft und dokumentiert werden.

Bereits im Juni 2024 betonte die BaFin in ihrer Aufsichtsmitteilung „*Hinweise zur Umsetzung von DORA im IKT-Risikomanagement und IKT-Drittparteien-Risikomanagement*“ das **Entfallen der bisherigen „IDV-Sonderbehandlung“**. Die Prüfung wird für alle eigenentwickelten Lösungen deutlich umfassender und strikter als bislang. Alle Fachbereichsanwendungen unterliegen denselben Prüf- und Dokumentationspflichten wie zentrale IT-Systeme, was die Anforderungen und Prüfintensität für eigenentwickelte Lösungen spürbar erhöht.

> **IDV-Tools rücken durch DORA in den Mittelpunkt:** Sie werden regulatorisch genauso behandelt wie zentrale IT-Anwendungen und müssen auch **wie jedes andere IKT-System bewertet, gesichert und kontrolliert** werden. Wer jetzt kein **stringentes IDV-Governance-System** etabliert, riskiert nicht nur **Sanktionen**, sondern auch **erhebliche operative Risiken**.

Schlanke Umsetzung: Jetzt zählt Mehrwert statt Formalismus

Mit der Einführung von DORA rückt die tatsächliche Wirksamkeit der Maßnahmen in den Mittelpunkt. Es gilt, die Ressourcen gezielt auf die Absicherung wesentlicher Risiken zu lenken, statt sich in umfangreichen Dokumentationen zu verlieren. Entscheidend ist ein **risikoorientierter Ansatz**, der pragmatisch ansetzt:

- **Kritikalität als Steuerungsgröße**: Statt für jede unkritische Anwendung einen vollständigen Dokumentationsprozess zu etablieren, sollten Unternehmen ihre Aufmerksamkeit auf die Anwendungen richten, die für die Geschäftskontinuität, die regulatorische Berichterstattung oder zentrale Kundenprozesse von hoher Bedeutung sind. So erhält beispielsweise ein aktuarielles Kernsystem zur Rückstellungsberechnung eine vollumfängliche Risikoanalyse, inklusive Quellcode-Prüfung und regelmäßigen Reviews, während ein rein internes Analyse-Tool mit einem pragmatischen Standardprozess ausreichend erfasst werden kann.
- **Schrittweise Standardisierung**: Die Einführung einheitlicher und schlanker Vorlagen für Risikoanalysen, Auslagerungsverträge und IDV-Dokumentationen unterstützt eine effiziente und konsistente Bearbeitung über alle Bereiche hinweg. Ein klar strukturierter Fragebogen zur IDV-Risikoanalyse, der direkt im

Fachbereich genutzt werden kann, stellt hier ein wirksames Instrument dar, um den Aufwand zu reduzieren und die Compliance sicherzustellen.

- **Synergien nutzen**: Viele Anforderungen aus DORA lassen sich nahtlos in bestehende Managementsysteme wie das Risikomanagement (gemäß Solvency II, MaRisk und ISO 31000), das Information Security Management (ISO 27001) oder das Business Continuity Management (ISO 22301) integrieren. Bestehende Notfalltests können beispielsweise gezielt um DORA-relevante IKT-Szenarien erweitert werden, ohne neue Parallelstrukturen aufzubauen. Entscheidend für eine nachhaltige DORA-Umsetzung ist ein holistischer Risikomanagement-Ansatz, der sämtliche Unternehmensbereiche einbindet und das verbreitete Silo-Denken konsequent aufbricht.
- **Praktikable Ausnahmeregelungen:** Auch unter DORA ist der Einsatz von Produktionsdaten in Testumgebungen möglich – allerdings nur nach einem formalisierten, nachvollziehbaren Genehmigungsprozess. Ein digitaler Freigabe-Workflow, beispielsweise über ein Ticketsystem, kann hier eine einfache und wirksame Lösung bieten.

Vom Regeldruck zur Chance: DORA nutzen und Wettbewerbsvorteile schaffen

DORA ist längst nicht mehr bloß ein regulatorisches Zukunftsthema – es ist **Gegenwart**. Es bietet auch die Chance, operative Schwächen sichtbar zu machen, Prozesse zu standardisieren und das Risikobewusstsein unternehmensweit zu stärken.

> Eine **schlanke, risikoorientierte Umsetzung von DORA** fokussiert sich auf die tatsächliche **Risikominderung** und **nachhaltige Resilienzsteigerung**. Entscheidend ist, dass die Maßnahmen im Unternehmensalltag **Wirkung entfalten** und nicht in Formalismus erstarren.

Sie möchten Ihr Unternehmen fit für DORA machen? Sprechen Sie uns an und tauschen Sie sich in den Kommentaren aus.

Dea Dubovci

Senior Consultant
Geschäftsfeld
Risikomanagement

dea.dubovci@cominia.de
+49 152 09502056

Dr. Mischa Pupashenko

Principal & Geschäfts-
feldverantwortlicher
Risikomanagement

mischa.pupashenko@cominia.de
+49 152 08437644

Literaturhinweise

BaFin Informationsseite: „DORA“

BaFin Publikation (2024): Aufsichtsmitteilung Umsetzungshinweise DORA.

BaFin Publikation (2025): Änderungen bei den aufsichtlichen Anforderungen an die IT.

BaFin Publikation (2025): Vorbereitung auf DORA: "Zacken zugelegt".

Digital Operational Resilience Act (DORA) | Updates, Compliance, Training:

EIOPA-IKT-Guidelines: Leitlinien zu Informations- und Kommunikationstechnologien (IKT) und Sicherheitsrisiken für Versicherungsunternehmen.

ISO 22301:2019: Security and resilience – Business continuity management systems – Requirements.

ISO 31000:2018: Risk management – Guidelines.

ISO/IEC 27001:2022: Information technology – Security techniques – Information security management systems – Requirements.

MaRisk: Mindestanforderungen an das Risikomanagement (MaRisk), BaFin, Rundschreiben 10/2021 (BA) vom 29.06.2021.

Richtlinie 2009/138/EG (Solvency II): Richtlinie des Europäischen Parlaments und des Rates vom 25. November 2009 über die Aufnahme und Ausübung der Versicherungs- und Rückversicherungstätigkeit.

VAIT: Versicherungsaufsichtliche Anforderungen an die IT (VAIT), BaFin, Rundschreiben 10/2018 (VAIT).

Verordnung (EU) 2022/2554: Verordnung des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor (DORA), Amtsblatt der EU, L 333/1.