GRM® Global Regulation

# Last Exit Brooklyn

## DORA Deepening

Julius Düwel
Dr. Waldemar Grudzien
Nadine Hofmann
Farahnoz Mirboboeva

Juni 2025
White Paper

## Anwendungsbereich

Mit der seit dem 17. Januar 2025 angewendeten DORA hat die Europäische Union eine Regulierung für die Themen Cybersicherheit, IKT-Risiken und digitale operationale Resilienz im Finanzsektor geschaffen. Diese Verordnung trägt wesentlich dazu bei, den europäischen Finanzmarkt gegenüber Cyberrisiken und Vorfällen der Informations- und Kommunikationstechnologie zu stärken. Außerdem führt DORA verschiedene, bereits bestehende Anforderungen an Finanzunternehmen in punkto Cybersicherheit, IT-Risiken und digitale Resilienz zusammen.

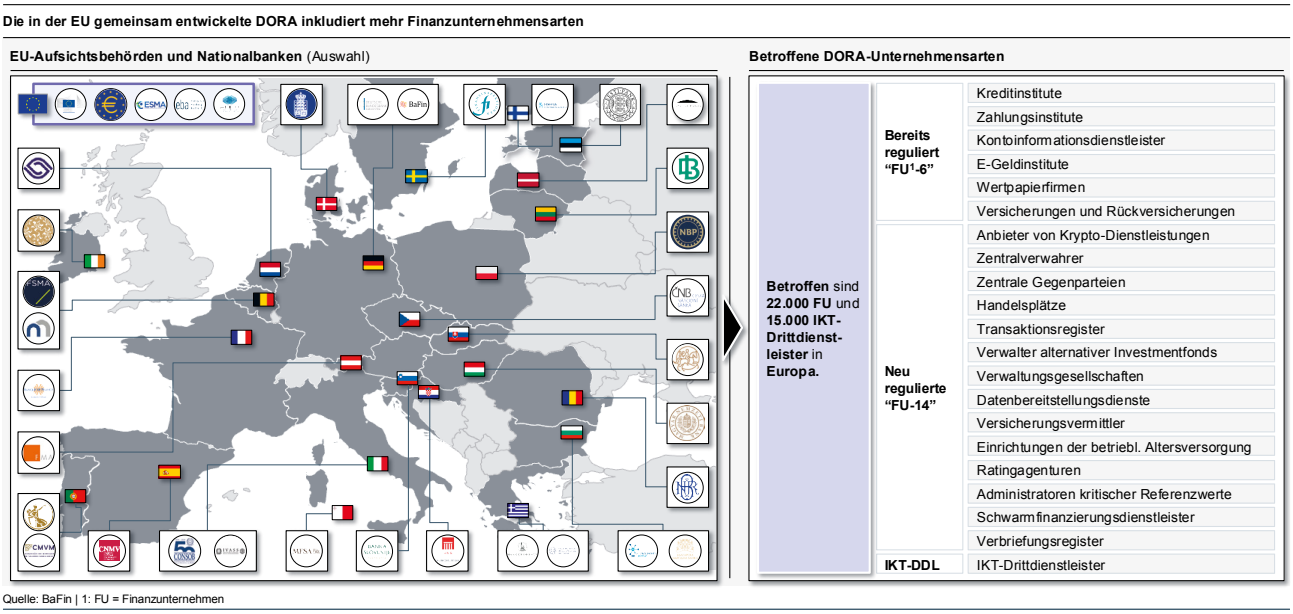



*Abbildung 1: DORA adressiert 21 Unternehmensarten in Europa, Deutschland ist geteilt*

Neben dem eigentlichen Verordnungstext werden die Inhalte der DORA durch weitere delegierte Rechtsakte in wen vorbereitete Gruppen von Betroffenen (Abbildung 1):

1. Finanzunternehmen aus dem XAIT-Aufsichtsregime (FU-6),

2. Finanzunternehmen, deren IT zum ersten Mal beaufsichtigt wird (FU-14),

Die erste Gruppe ist seit der ersten Finanzkrise im Jahre 2008 und der damit einhergehenden Verschärfung der Aufsichtsregime prüfungserfahren. DORA bedeutet für diese aus sechs Arten von Finanzunternehmen bestehende Gruppe zwar eine weitere Verschärfung der Sicherheitsanforderungen, jedoch ist es für diese Gruppe seit vielen Jahren eine gelebte Praxis, bestehend aus Prüfungsankündigung, Prüfung, Mängelbeseitigung, Nachschauprüfung und operativem IT-Betrieb bis zur nächsten Prüfungsankündigung in zwei bis fünf Jahren.

Der Erfahrungshorizont dieser Gruppe mit dem Regulator und der Aufsicht wird nicht zuletzt aus Sanktionserfahrungen gespeist wie beispielsweise:

- Citibank N.A., Filiale Frankfurt am Main: Die BaFin hat die Sicherstellung der ordnungsgemäßen Geschäftsorganisation und eine regelmäßige Berichtspflicht zum Fortschritt der Mängelabstellung angeordnet[1].
- Deutsche Bank AG: Die BaFin setzt Geldbuße in Höhe von 23,05 Millionen Euro gegen die Deutsche Bank AG fest. Das Unternehmen hatte unter anderem im Zusammenhang mit dem Vertrieb von Derivaten gegen organisatorische Pflichten des Wertpapierhandelsgesetzes (WpHG) verstoßen[2].
- SECB Swiss Euro Clearing Bank GmbH: BaFin ordnet Sicherstellung einer ordnungsgemäßen Geschäftsorganisation an. Darüber hinaus muss die Bank zusätzliche Eigenmittelanforderungen einhalten, bis sie die organisatorischen Mängel beseitigt hat. Dies hat die Finanzaufsicht BaFin angeordnet[3].

Die zweite Gruppe betrifft Finanzunternehmen, die bisher durch die Finanzaufsicht nicht in ihrer IT beaufsichtigt worden sind. Diese 14 Arten von Finanzunternehmen müssen sich nun gemäß DORA-Regime ohne vorherige Erfahrungswerte auf eine vollumfängliche und gründliche Erstprüfung ihrer IT-Ausstattung vorbereiten. Während diese zweite Gruppe einen Arbeitsmodus zur Finanzaufsicht aus anderen Kontaktpunkten besitzt wie zum Beispiel Geldwäsche- oder Kreditprüfung, besteht bei der dritten Gruppe der IKT-Drittdienstleister bisher keine Arbeitsbeziehung zur Finanzaufsicht.

IKT-DDL werden somit zum ersten Mal durch die Finanzaufsicht geprüft. Diese Neuerung führt nicht nur zu hohen Aufwänden aus dem faktischen Inhalt der DORA heraus, sondern sie stellt auch eine psychologische Herausforderung für die Dienstleister dar, da sie durch eine fachfremde Behörde beaufsichtigt werden. Es kann davon ausgegangen werden, dass die großen Dienstleister der Banken und Versicherungen wie US-amerikanische Hyperscaler die Herausforderung DORA kraft ihrer technologischen Führerschaft, organisatorischen Professionalität und finanzieller Ausstattung gut bewältigen werden. Für die mittleren und kleineren IKT-DDL wird DORA jedoch mit einer enormen Steigerung der Compliance-Aufwände einhergehen.

Neben kritischen IKT-Drittdienstleistern müssen sich auch CIF-Lieferanten seriös zu DORA aufstellen.

Je nach organisatorischer Reife, finanzieller Stärke und dem Mindset eines IKT-DDL aus dieser Gruppe stehen diese Unternehmen vor der grundsätzlichen Frage der Reaktion auf die durch DORA abrupt steigenden Compliance-Aufwände: Verkauf, Merger oder Herstellung der DORA-Konformität. Die letztgenannte Lösungsoption bedeutet die konforme Umsetzung der DORA.

Das White Paper ist die dritte, vollständig überarbeitete Ausgabe unserer Reihe „Last Exit Brooklyn“ zur DORA. Es beschreibt im Folgenden die Auswirkungen der DORA-Regulierung entlang der Schwerpunktthemen der DORA: Risikomanagementrahmen, Drittparteienrisiko, Vorfallmanagement, Tests der Resilienz – alles im Lichte der IKT. In Ausführungen zur Schweiz als wichtigem Partner des EU-Finanzsektors und zu Großbritannien als Sitz von Brexit-Banken wird der DORA-Horizont um die Bedeutung für Auslagerungsverhältnisse erweitert.

# 1 DORA in Zahlen

Insgesamt wird die DORA durch weitere 14 Dokumente konkretisiert (Abbildung 2), davon acht Regulatory Technical Standards (RTS), zwei Implementing Technical Standards (ITS) und drei Guidelines (GL).

In der ersten Entwurfsstufe im Oktober 2024 umfasste die Kodifizierung der DORA insgesamt 1.003 Seiten, im November waren es 752 Seiten und im Dezember 679 Seiten. Derzeit beträgt die Seitenzahl 562 Seiten. Die Autoren rechnen bei allen finalisierten Dokumenten mit 330 bis 370 Seiten für die gesamte DORA. All diese Entwurfsstände mussten und müssen von allen Adressaten gelesen, analysiert, ausgewertet, verstanden und in einer adäquaten proportionalen Form umgesetzt werden.

**Übersicht über DORA und RTS[1], ITS[2], GL[3]-Vorgaben** — Final

| Kapitel | Bezeichnung/Artikel |
|---|---|
| 1 Allgemeine Bestimmungen | ▪ Artikel 1 bis Artikel 4 |
| 2 IKT[4]-Risikomanagement | ▪ Abschnitt I, Artikel 5<br>▪ Abschnitt II, Artikel 6 bis 16 |
| 3 IKT-Vorfallmanagement | ▪ Artikel 17 bis 23 |
| 4 Testen der digitalen Resilienz | ▪ Artikel 24 bis 27 |
| 5 Management des IKT-Drittpartnerrisikos | ▪ Abschnitt I, Artikel 28 bis 30<br>▪ Abschnitt II, Artikel 31 bis 44 |
| 6 Vereinbarungen zum Informationsaustausch | ▪ Artikel 45 |
| 7 Zuständige Behörden | ▪ Artikel 46 bis Artikel 56 |
| 8 Delegierte Rechtsakte | ▪ Artikel 57 |
| 9 Übergangs- und Schlussbestimmungen | ▪ Abschnitt I, Artikel 58<br>▪ Abschnitt II, Änderungen: Artikel 59 bis 64 |

Konkretisierende Dokumente

April 2025

| Artikel | Typ | Beschreibung und Kapitelzuordnung | |
|---|---|---|---|
| 11 (11) | GL 34 | Schätzung aggregierter jährlicher Kosten | 3 |
| 15, 16 (3) | RTS 86 | IKT-Risikomanagement | 2 |
| 18 (4) | RTS 83 | Klassifikation schwerwiegender Vorfälle | 3 |
| 20 a/b | RTS/ITS 33 | Meldung/Berichterstattung schwerwieg. IKT-Vorfälle | 3 |
| 26 (11) | RTS 29 | Spezifizierung von TLPT[5] | 4 |
| 28 (9) | ITS 85 | Informationsregister inkl. Template | 5 |
| 28 (10) | RTS 84 | Policy zu IKT-Vereinbarungen mit Dritten | 5 |
| 30 (5) | RTS 53 | Unterauftragsvergabe kritischer Funktionen | 5 |
| 31 (6) | GL | Kriterien für kritische IKT-DDL, Art. 31(6) | 5 |
| 32 (7) | GL 36 | Zusammenarbeit ESA[6] und CAs[7] | 5 |
| 41 (1), a, b, d | RTS 35 | Harmonisierung Bedingungen Überwachungstätigkeiten | 5 |
| 41 (1), c | RTS 54 | Zusammensetzung gemeinsame Untersuchungsteams | 5 |
| 43 (2) | GL | Überwachungsgebühren bei kritischen IKT-DDL | 5 |

Quelle: EU DORA | ESA (drei Europäische Aufsichtsbehörden für den Finanzsektor: EBA, EIOPA und ESMA) | 1: RTS = Regulatorische technische Standards | 2: ITS = Implementierung technischer Standards | 3: GL = Guidelines | 4: IKT = Informations- und Kommunikationstechnologie | 5: TLPT = Threat-Led Penetration Testing | 6: ESA = Europäisches Finanzaufsichtssystem | 7: CA = Zuständige nationale Behörde

*Abbildung 2: Aufbau der DORA mit 14 konkretisierenden Dokumenten*

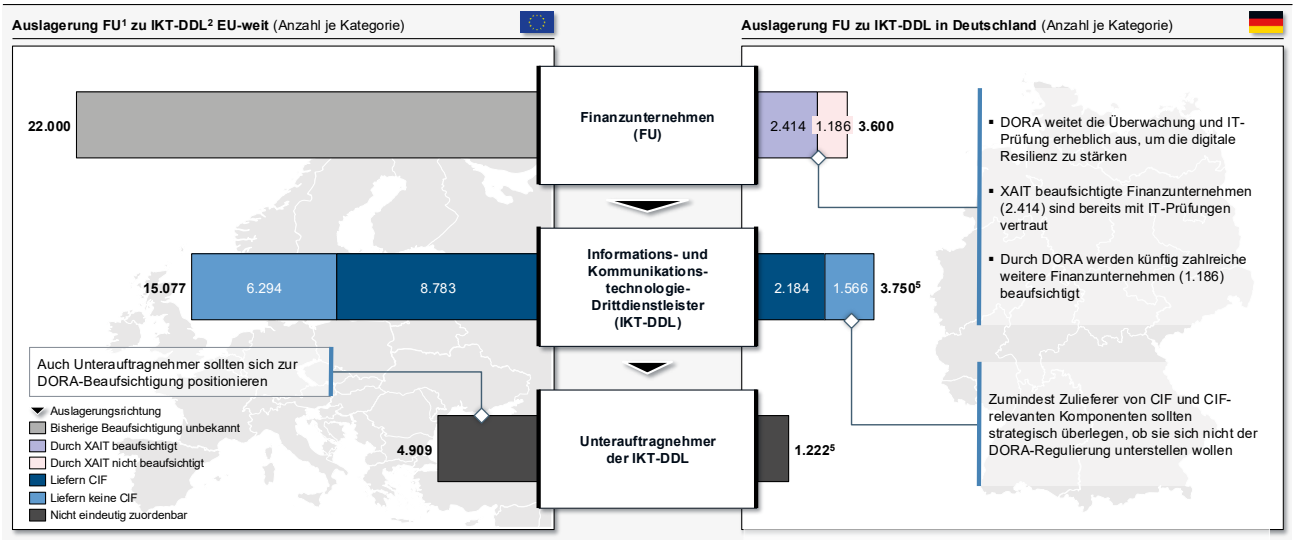
Auch wenn DORA zuerst mit Banken und Versicherungen in Verbindung gebracht wird, sind neben diesen zwei noch 18 weitere Arten von Finanzunternehmen adressiert. Zudem werden mit der DORA zum ersten Mal IKT-DDL als Zulieferer der 20 Arten von Finanzunternehmen Objekte der Finanzaufsicht.

Die BaFin hat bis zur Anwendung der DORA sechs der 20 Finanzunternehmensarten bzw. nach eigenen Angaben 2.414 Finanzunternehmen[4] mittels XAIT (zusammenfassendes Akronym für BAIT, KAIT, VAIT und ZAIT) und MaX (zusammenfassendes Akronym für MaRisk, MaGo und MaComp) adressiert. Mit der DORA wird dieser Adressatenkreis in Deutschland auf „über 3.600“ Finanzunternehmen[5] erweitert, sodass aufgerundet 1.200 neu beaufsichtigte Finanzunternehmen hinzukommen. Diese werden in Deutschland erstmals einer IT-Aufsicht unterstellt (Abbildung 3).

Für die EU geben die ESAs die Anzahl der IKT-DDL mit 15.077 an, mit Weiterverlagerung steigt die Anzahl der IKT-DDL auf 19.986. Davon liefern 8.783 IKT-DDL der europäischen Finanzindustrie kritische oder wichtige Funktionen (CIF)[6]. Nur diese werden in den Anwendungsbereich der DORA fallen. Weder die ESAs noch die nationalen

Aufsichtsbehörden nennen die Anzahl der IKT-DDL pro Mitgliedsstaat. Die Autoren haben deshalb diese Zahl deutscher IKT-DDL im Verhältnis der Wirtschaftskraft Deutschlands zur EU auf 3.750 bestimmt. Im Ergebnis müssen in Deutschland neben den Finanzunternehmen der FU-6-Gruppe ca. 1.200 weitere Finanzunternehmen der FU-14-Gruppe die DORA erfüllen. Auch die ca. 3.750 IKT-DDL müssen sich zur DORA verhalten. Nur mit Konformität können auch die neuen Aufsichtsobjekte eine mögliche Prüfung ohne schwerwiegende Sanktionen der Finanzaufsicht überstehen.

**Zahlenwerk Finanzunternehmen (FU) und Informations- und Kommunikationstechnologie-Drittdienstleister (IKT-DDL) vor und mit DORA auf Ebene der EU und DE in 2025**




Quelle: GRM | 1: FU = Finanzunternehmen | 2: IKT-DDL = Informations- und Kommunikationstechnologie-Drittdienstleister | 3: DORA = Digital Operational Resilience Act | 4: XAIT = Überbegriff für Bankaufsichtliche / Kapitalverwaltungsaufsichtliche / Versicherungsaufsichtliche / Zahlungsdienstaufsichtliche Anforderungen an die IT | 5: ESA und BaFin veröffentlichen keine Zahlen auf Einzelstaatenebene, GRM-Expertenschätzung auf Basis der Wirtschaftskraft Deutschlands zur EU

*Abbildung 3: DORA erschafft neuen lukrativen Markt für Sicherheitsdienstleistungen*

Der Katalog möglicher Sanktionen ist weit gefasst und die BaFin agiert klug in der Wahl ihrer Mittel: Sie wählt üblicherweise Sanktionen für Finanzunternehmen, die Wirkung entfalten. Beispiele sind neben den „Klassikern“ Anordnung eines Bußgeldes, Einsetzen eines Sonderbeauftragten und Abwahl des verantwortlichen Mitglieds des Vorstands auch die Beschränkung des Neukundengeschäfts, die Beschränkung des Neukreditgeschäfts oder die vorübergehende Aussetzung eines neuen Geschäftsfeldes bis zur Beseitigung der festgestellten Mängel. Die Art der Sanktionen wird gesondert für das Aufsichtsobjekt bestimmt.

IKT-Drittdienstleister, die durch die ESAs nicht als kritisch eingestuft werden, müssen folgenden Aspekt bedenken: Im Sinne der DORA als kritisch klassifizierte IKT-DDL verfügen mit der DORA-Konformität über einen Ausweis ihrer durch die Finanzaufsicht anerkannt hohen Sicherheit. Im Sinne der DORA nicht kritische IKT-DDL müssen nicht den Nachweis der DORA-Konformität erbringen und verfügen deshalb auch nicht über diese Auszeichnung der operationellen Resilienz und Sicherheit. Es bleibt abzuwarten, wie sich die Finanzunternehmen im Markt orientieren werden. Die Autoren prognostizieren einen Vorteil der DORA-kritischen Dienstleister im Markt. Diese mögliche Entwicklung antizipierend bietet §31 Absatz 11 DORA denjenigen IKT-Dienstleistern, die nicht als kritisch eingestuft sind, die Möglichkeit, diesen Status zu beantragen.

## 2 IKT-Risikomanagementrahmen

Der IKT-Risikomanagementrahmen ist kodifiziert durch Kapitel II (Artikel 5 bis 16) der DORA und durch das konkretisierende RTS 86 „Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und den vereinfachten IKT-Risikomanagementrahmen“. Das RTS 86 konkretisiert die allgemeinen Vorgaben der DORA in detaillierte Anforderungen zu den wesentlichen Themen eines Informationssicherheitskatalogs.

Gemäß Artikel 6 Absatz 1 fordert DORA „einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen, der Teil des Gesamtrisikomanagement-systems ist und es ermöglicht, IKT-Risiken schnell, effizient und umfassend anzugehen und ein hohes Niveau an digitaler operationaler Resilienz zu gewährleisten. Nach Artikel 6 (2) DORA „umfasst der IKT-Risikomanagementrahmen mindestens Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle und -Tools, die erforderlich sind, um alle Informations- und IKT-Assets, einschließlich Computer-Software, Hardware und Server, ordnungsgemäß und angemessen zu schützen sowie um alle relevanten physischen Komponenten und Infrastrukturen, wie etwa Räumlichkeiten, Rechenzentren und ausgewiesene sensible Bereiche zu schützen, damit der angemessene Schutz aller Informations- und IKT-Assets vor Risiken, einschließlich der Beschädigung und des unbefugten Zugriffs oder der unbefugten Nutzung, gewährleistet ist“.

Der IKT-Risikomanagementrahmen soll sich somit in das bereits vorhandene Risikomanagementsystem des Finanzunternehmens und damit in die vorhandene Aufbau- und Ablauforganisation (Governance) eingliedern. Die weiteren Anforderungen an den IKT-Risikomanagementrahmen aus Artikel 6 sind:

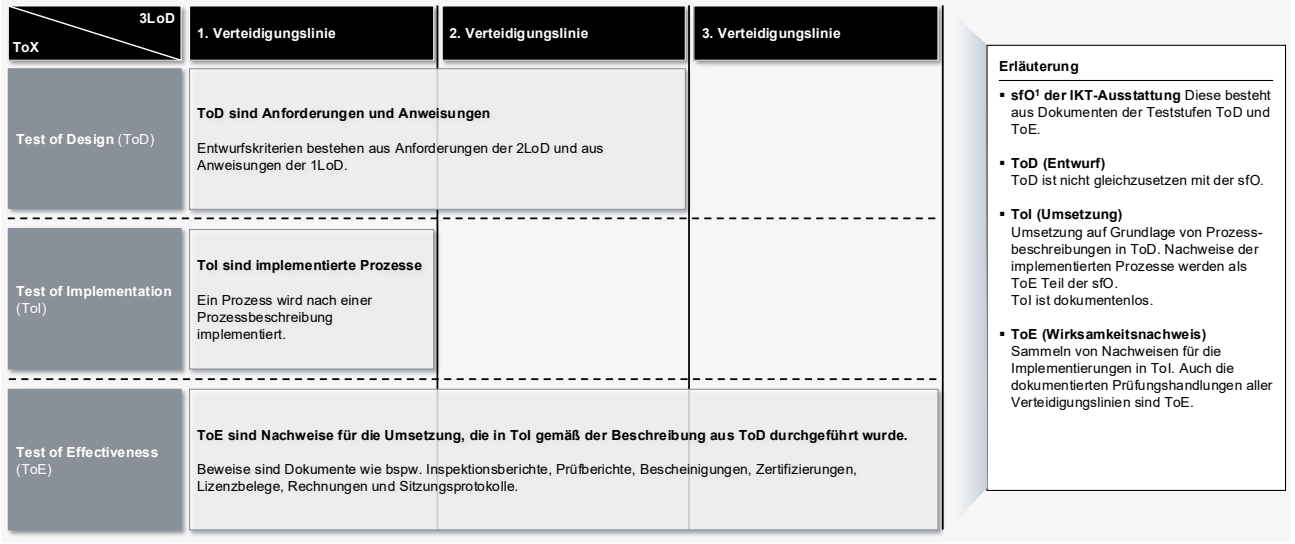
Der IKT-Risikomanage-mentrahmen besteht aus vorhandenen Komponenten – Aufbau neuer Strukturen ist nicht notwendig.

1) Das Finanzunternehmen ist zu IKT-Risiken und dem IKT-Risikomanagement-rahmen jederzeit rechenschaftspflichtig gegenüber der Aufsicht. (Absatz 3)
2) Es muss eine unabhängige Kontrollfunktion für das Management und die Überwachung des IKT-Risikos installiert werden. (Absatz 4); Diese Funktion kann ausgelagert werden. (Absatz 10)
3) Der IKT-Risikomanagementrahmen wird mindestens einmal jährlich sowie bei Auftreten schwerwiegender IKT-bezogener Vorfälle und nach aufsichtsrechtlichen Anweisungen oder Feststellungen dokumentiert und überprüft. (Absatz 5)
4) Im Einklang mit dem Revisionsplan des betreffenden Finanzunternehmens ist der IKT-Risikomanagementrahmen von Finanzunternehmen regelmäßig einer internen Revision durch Revisoren zu unterziehen. (Absatz 6)
5) Folgemaßnahmen zu Feststellungen aus internen Audits. (Absatz 7)
6) Der IKT-Risikomanagementrahmen umfasst eine Strategie für die digitale operationale Resilienz, in der dargelegt wird, wie der Rahmen umgesetzt wird. (Artikel 8)
7) Strategie zur Nutzung mehrerer IKT-DDL (Kann-Bestimmung, Absatz 9)

Die IKT-Risikomanagementfunktion ist eine Erweiterung der aus der BAIT bekannten ISB-Funktion um das Risikomanagement.

Eine Anforderung muss geplant und implementiert, ihre Wirksamkeit muss nachgewiesen werden. Die formelle Abbildung dieser drei Zustände erfolgt in den drei Teststufen Design, Implementierung und Effektivitätsnachweis als Test of Design (ToD), Test of Implementation (ToI) und Test of Effectiveness (ToE). Die Teststufen werden durch verschiedene Bereiche einer Organisation bereitgestellt. Die 1LoD setzt Prozesse um und ist damit für das ToI verantwortlich. Die 2LoD und auch die 1LoD stellen die Anforderungen und triggern damit ToD. Die interne Revision bildet die 3LoD und liefert den finalen Beweis, dass ein geplanter (ToD) und umgesetzter (ToI) Prozess wirksam (ToE) ist. Aber auch die ersten beiden Verteidigungslinien steuern über die 1st- und 2nd Line-Kontrollen ihren Teil zur Wirksamkeitsprüfung bei. In diesem in Abbildung 4 illustrierten ToX-3LoD-System kann jedes Artefakt definiert und mit einer Verantwortlichkeit versehen werden. Dadurch werden jede Anforderung, jeder Prozess und jede Evidenz überprüfbar und nachvollziehbar.

**Grundprinzipien des ToX/3LoD-Systems der IT-Ausstattung**




Quelle: GRM | 1: sfO = schriftlich fixierte Ordnung

*Abbildung 4: ToX-3LoD-Ordnungsschema für Finanzunternehmen und IKT-DDL*

Wie oben ausgeführt sollte sich der IKT-Risikomanagementrahmen in das bereits vorhandene Gesamtrisikomanagementsystem einfügen. Finanzunternehmen der FU-6-Gruppe sind bereits in der IT-Ausstattung reglementiert und müssen aus XAIT heraus über ein Informationssicherheitsmanagementsystem (ISMS) verfügen. Ein ISMS besteht aus Richtlinien, Verfahren, Leitlinien und zugehörigen Ressourcen und Aktivitäten, die von einer Organisation gemeinsam verwaltet werden, um ihre Informationsressourcen zu schützen. Der weltweit meistverwendete Standard für ein ISMS ist der ISO-Standard 27001. In Deutschland bekannt ist zudem eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz des BSI. Ein nach dem ISO 27001-Standard aufgebautes ISMS erfüllt bereits viele Anforderungen eines IKT-Risikomanagementrahmenwerkes nach DORA, allerdings nicht alle.

Viele Finanzunternehmen nutzen auch das NIST Cybersecurity Framework (CSF)[7]. Das NIST CSF besteht aus einer Reihe von Richtlinien, die Organisationen eine Orientierungshilfe bieten, ihre Fähigkeit zur Prävention, Erkennung und Reaktion auf Cybersicherheitsrisiken zu bewerten und zu verbessern. Hierzu bietet das CSF Online-

Ressourcen der NIST an, die Anleitungen zu Verfahren, Kontrollen und Maßnahmen für die Umsetzung der Sicherheitsziele im Umgang mit Cyberrisiken bieten.

Der Kern des CSF ist der CSF Core. Dieser besteht aus einer Hierarchie von Funktionen, Kategorien und Unterkategorien, die jedes Ziel und die möglichen Maßnahmen der Cybersicherheit detailliert beschreiben. In der aktuellen Version 2.0 ist das CSF in sechs Funktionen unterteilt: Steuern, Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen. Beide Rahmenwerke – ISO 27001 und CSF 2.0 – sind in Abbildung 5 exemplarisch an den Artikeln der DORA gespiegelt.

**Industriestandards unterstützen DORA-Umsetzung**

| DORA | ISO 27001 | CSF2.0 Category Identifier | RTS/ITS |
|---|---|---|---|
| **Art. 5: Governance und Organisation** | **HLS: 6.1, 8.2, 8.3** | **…** | ▪ RTS 86, Art. 1: Gesamtrisikoprofil und Komplexität<br>▪ RTS 86, Art. 2: RL, Verfahren, Tools für IKT-Sicherheit<br>▪ RTS 86, Art. 19: Richtlinien für Personalpolitik<br>▪ RTS 86, Art. 27: Bericht Überprüfung des IKT-RMR |
| 5 (1): Governance und Kontrollrahmen | A.8 | … | |
| 5 (2): Leitungsorgan: Verantwortung | HLS 5.1, A.5.31 | GV.OC, GV.PO | |
| 5 (3): Kontrollfunktion IKT-DDL | HLS 9 | GV.RR | |
| 5 (4): Leitungsorgan: Kenntnisse/ Fähigkeiten | … | … | |
| **Art. 6: IKT-Risikomanagementrahmen** | **HLS: 6.1, 8.2, 8.3** | **…** | ▪ RTS 86, Art. 3: IKT-Risikomanagement<br>▪ RTS 86, Art. 4: RL für das Management von IKT-Assets<br>▪ RTS 86, Art. 5: Verfahren für das Management von IKT-Assets<br>▪ RTS 86, Art. 27: Bericht Überprüfung des IKT RMR |
| 6 (1): IKT-Risikomanagementrahmen | A.5.9 bis A.5.13. | … | |
| 6 (2): Strategien, Leit-/ Richtlinien, Verfahren | A.5.1 | GV.RM | |
| 6 (3): IKT-Risiken | … | … | |
| 6 (4): IKT-Risikomanagement-Funktion | A.5.2, A.5.3 | … | |
| 6 (5): Überprüfung des IKT-RM-Rahmens | HLS 9 | … | |
| 6 (6): Interne Revision des IKT-RM-Rahmens | HLS 9.2, A.5.35 | … | |
| 6 (7): Follow-Up zu (6) | … | … | |
| 6 (8): Strategie digitale operationelle Resilienz | … | GV.OV | |
| 6 (9): Strategie mehrere IKT-DDL | A.5.19 bis A.5.23 | … | |
| 6 (10): Auslagerung der Überprüfung | … | … | |
| **Art. 7: IKT-Systeme, -Protokolle und -Tools** | **HLS 6.1, A.8** | **…** | ▪ RTS 86, Art. 2: RL, Verfahren, Tools für IKT-Sicher.<br>▪ RTS 86, Art. 9: Kapazitäts- und Leistungsmanagm.<br>▪ RTS 86, Art. 15: IKT-Projektmanagement<br>▪ RTS 86, Art. 16: Beschaffung, Entwicklung, Wartung |
| a) – b): …sind verhältnismäßig und zuverlässig | HLS 4, A.5.4 | … | |
| c) – d): …ausreichende Kapazitäten und technologisch resilient | A.8.6 | … | |

*Abbildung 5: IKT-Risikomanagement am Beispiel der Artikel 5 bis 7 – gespiegelt an ISO 27001 und CSF 2.0*

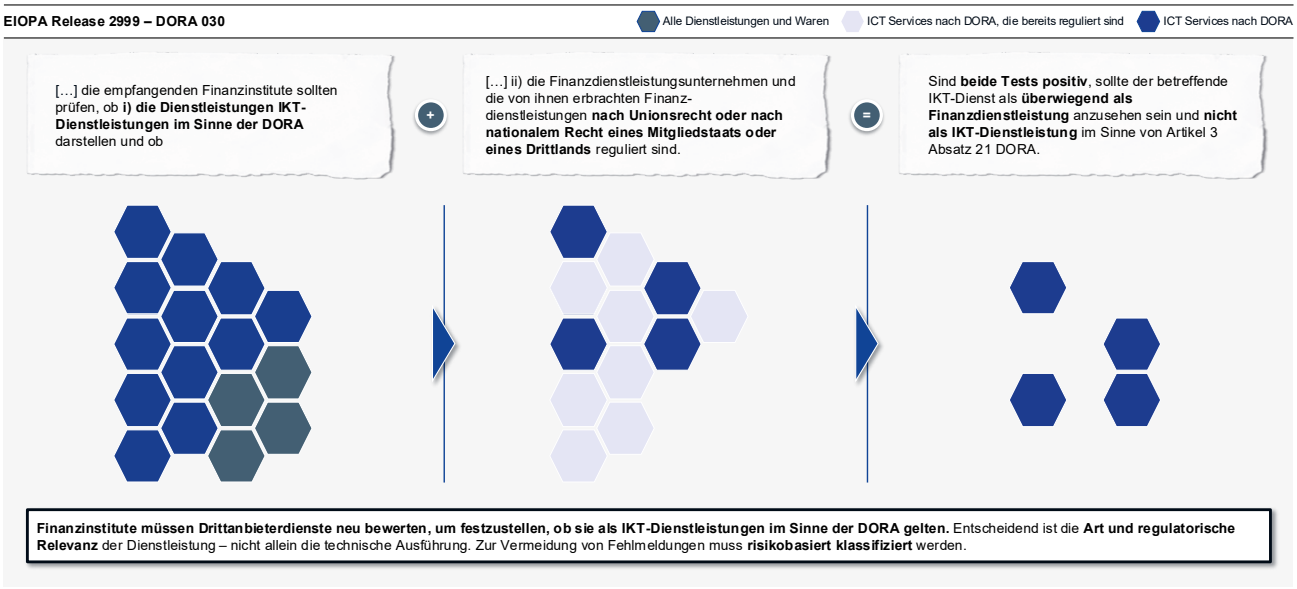
## 3 Management des IKT-Drittparteienrisikos

Das Management des IKT-Drittparteienrisikos muss aus der Außen- und der Innenansicht gelesen werden: Die Außenansicht steuert die ESA durch die Einstufung eines IKT-Drittdienstleisters als kritisch im Sinne der DORA. Die Innenansicht wird bestimmt durch die Vertragsbeziehung zwischen Finanzunternehmen und IKT-DDL. Zunächst müssen Finanzunternehmen für sich definieren, was kritische oder wichtige Funktionen (CIF) als auch diese Funktionen unterstützende IKT-DDL sind. Verträge mit CIF-unterstützenden IKT-DDL unterliegen strengeren Anforderungen bei Überwachung, Sicherheitsmaßnahmen und Notfallplänen.

Mit dem Wegfall der BAIT muss ein separates Beurteilungsschema für die Identifizierung von kritischen oder wichtigen Funktionen bestehen, da DORA nur noch zwischen kritischen oder wichtigen bzw. nicht kritischen oder wichtigen Funktionen unterscheidet und die Wesentlichkeitsbeurteilung abschafft. Gemäß Art. 3 (22) DORA sind Funktionen kritisch oder wichtig, wenn ihr Ausfall erhebliche Auswirkungen auf die finanzielle Leistungsfähigkeit, die Fortführung des Geschäftsbetriebs oder regulatorischer Natur hätte. Die implementierungstechnischen Standards (ITS) für das Informationsregister verlangen zusätzliche Datenpunkte für die kritischen oder wichtigen Funktionen

unterliegenden Verträge, die den Informationsanforderungen an Auslagerungen nach EBA sehr ähnlich sind. Auch entstammt die vormalige Definition des Begriffes kritisch oder wichtig aus dieser.

Ob man zur Vereinfachung die Definitionen der MaRisk mit denen der DORA gleichsetzen kann, wird unter anderem von der Methode zur Identifizierung von kritischen oder wichtigen Funktionen im IKT-Risikomanagement beeinflusst. Die EBA hat ihre Richtlinie für IKT- und Sicherheitsrisikomanagement aufgrund von DORA abgeändert. Dazu gehört die Eingrenzung des Anwendungsbereiches, durch die die Leitlinie nur noch für Finanzinstitute gilt, die unter die DORA fallen. Die Leitlinie wurde insofern angepasst, um Überschneidungen mit der DORA zu vermeiden, die pan-europäische Mindestanforderungen stellt. Weitere Änderungen von Richtlinien könnten folgen, wie zum Beispiel die Anpassung der EBA-Richtlinie zu Auslagerung (Abbildung 6).




Quelle: EIOPA, GRM

*Abbildung 6: Ausschluss von Finanzservices zur Vermeidung von Doppelregulation nach EIOPA*

Ist ein Vertrag mit einem IKT-DDL möglicherweise an der Leistungserbringung einer kritischen oder wichtigen Funktion beteiligt, müssen all diese Drittverträge überprüft werden, um kritische oder wichtige Funktionen unterstützende Dienstleistungen zu identifizieren und zu priorisieren. Diese Verträge müssen neu verhandelt werden für zusätzliche Anforderungen wie Prüfungsrechte, IKT-Sicherheitsmaßnahmen, Notfallpläne und Regelungen zur Unterauftragsvergabe in Form von Addenden oder Vertragsneuerungen. Zusätzlich müssen Verträge für kritische oder wichtige Funktionen eine regelmäßige, automatisierte Berichterstattung über Vorfälle und Risiken beinhalten, was den Aufwand und die Komplexität im Vertragsmanagement erhöht.

Wie bereits beschrieben (siehe Abbildung 2), ist die DORA trotz Inkrafttreten am 17. Januar 2025 noch nicht vollständig. Nachdem die Europäische Kommission den Entwurf der ITS 28 aufgrund[8] von Bedenken im Sommer 2024 hinsichtlich der vorgeschlagenen Identifizierungsanforderungen für Drittanbieter von IKT-Dienstleistungen abgelehnt hatte, hat sie am 21. Januar 2025 den Entwurf der RTS 53 zur Unterauftragsvergabe

im Rahmen des Gesetzes abgelehnt, da sie zu dem Schluss gekommen ist, dass einige Bestimmungen über das Mandat hinausgehen, das den Europäischen Aufsichtsbehörden (ESAs) in Artikel 30 Absatz 5 DORA übertragen wurde. Die Kommission beanstandete insbesondere Artikel 5 des Entwurfs der RTS, in dem die Bedingungen für die Vergabe von Unteraufträgen im Zusammenhang mit der Kette von IKT-Unterauftragnehmern, die Dienste zur Unterstützung kritischer oder wichtiger Funktionen erbringen, festgelegt waren. Sie würden Verpflichtungen einführen, die nicht in direktem Zusammenhang mit den in Artikel 30 Absatz 5 der DORA festgelegten Bedingungen für die Vergabe von Unteraufträgen standen. Daher forderte die Kommission dessen Streichung[9].

## 4 Vorfallmanagement

Mit der DORA wird ein harmonisierter Rahmen für die Meldung von Vorfällen eingeführt, der die Meldung aller IKT-bezogenen Vorfälle vorschreibt, die sich auf kritische oder wichtige Funktionen auswirken. Diese harmonisierte Berichterstattung über Vorfälle ersetzt seit dem 17. Januar 2025 das Meldeverfahren für schwerwiegende Betriebs- und Sicherheitsvorfälle bei Zahlungsdienstleistern gemäß PSD2. Nach DORA müssen folgende Vorfallsarten gemeldet werden:

a) Ein erfolgreicher, böswilliger und unbefugter Zugriff auf das Netzwerk und die Informationssysteme des Finanzunternehmens, d.h. mit einem potenziellen oder erfolgten Datenleck, muss sofort gemeldet werden.
b) Unterbrechung von IKT-Diensten oder -Systemen, die kritische oder wichtige Funktionen unterstützen.
c) Beeinträchtigung genehmigungspflichtiger regulierter Finanzdienstleistungen.

Vorfallmanagement ist Sache der Geschäftsfunktionen, nicht nur von Compliance und IT.

Die Vorfallklassen b) und c) sind meldepflichtig, wenn mindestens zwei der folgenden sechs Kriterien betroffen sind:

1) Kunden, finanzielle Gegenparteien oder Transaktionen
2) Datenverlust
3) Reputationsschaden
4) Dauer und Ausfallzeit des Dienstes
5) Geografische Ausbreitung
6) Wirtschaftliche Auswirkungen

Folgende Meldefristen müssen beachtet werden (Abbildung 7):

- Erstmeldung: Innerhalb von 24 Stunden nach Entdeckung des Vorfalls und innerhalb von 4 Stunden nach Einstufung des Vorfalls als meldepflichtig.
- Zwischenbericht: Innerhalb von 72 Stunden nach der Erstmeldung.
- Abschlussbericht: Innerhalb eines Monats nach dem Zwischenbericht.

Traditionell wurden die Widerstandsfähigkeit der IKT und die Einhaltung der regulatorischen Vorschriften als technisch-organisatorische Themen betrachtet. DORA erweitert jedoch die Verantwortlichkeit über die Compliance- und IT-Teams hinaus auf die Geschäftsfunktionen, wodurch die Notwendigkeit entsteht, die betriebliche Ausfallsicherheit ins Zentrum des

Finanzunternehmens einzubetten. Dies bringt eine Reihe von Herausforderungen mit sich:

- Identifizierung kritischer Systeme und ihrer Rolle in der Organisation.
- Einbindung kritischer und wichtiger Funktionen in den organisatorischen Rahmen.
- Definition eines Rahmens für die lokale, von der global agierenden Zentrale unabhängigen Unternehmensverantwortung.
- Entwicklung von Echtzeit-Überwachungs-Dashboards zur Erkennung von Vorfällen.
- Einbindung eines breiten Spektrums von Interessenvertretern, von IT und Compliance bis hin zu Risiko, Betrieb und Geschäftsfunktionen.

**Möglicher Prozess für das Vorfallmanagement zur Umsetzung**

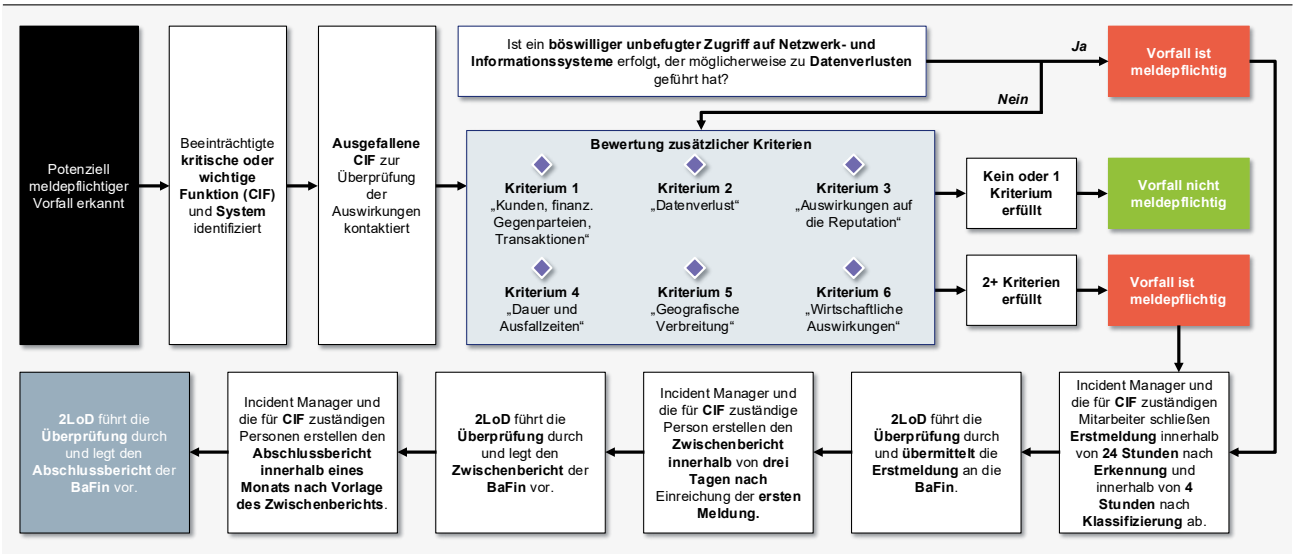



*Abbildung 7: Prozess im Vorfallmanagement für Erstmeldung, Zwischen- und Abschlussbericht*

Dieser Wandel erfordert eine Kultur der Verantwortlichkeit, die sicherstellt, dass die Geschäftsfunktionen nicht nur informiert, sondern auch aktiv in das Risikomanagement einbezogen werden. Resilienz ist damit nicht mehr nur ein IT- oder Compliance-Thema. Es ist ein Thema, das die gesamte Organisation betrifft, von der IT bis zu allen Geschäftsfunktionen. Eine funktionsübergreifende Zusammenarbeit ist erforderlich. Cybersicherheits-, Compliance- und IT-Teams können nicht länger in Silos arbeiten - das Unternehmen muss neben diesen Funktionen Verantwortung übernehmen, um die Einhaltung der Vorschriften zu gewährleisten.

Beispiele für die Verankerung einer Kultur der Verantwortlichkeit für Geschäftsfunktionen sind:

a) Key Risk Indicators (KRIs) und Key Performance Indicators (KPIs) auch auf Unternehmensebene, um die Verantwortlichkeit für die Widerstandsfähigkeit zu gewährleisten.
b) Durchführung von funktionsübergreifenden Table-Top-Übungen, die den Prozess simulieren.
c) Verknüpfung von Leistungsprämien oder KPIs mit den Fristen für die Bewertung von Vorfällen und die rechtzeitige Meldung an die BaFin.

## 5 DORA für IKT-Drittdienstleister

Wichtig für IKT-Drittdienstleister sind Kapitel 5 „Management des IKT-Drittparteienrisikos“ der DORA sowie die begleitenden Dokumente RTS 53 zur „Harmonisierung der Bedingungen für die Durchführung der Aufsichtstätigkeiten“, Guidelines zur „Festlegung der Kriterien für die Einstufung von IKT-Drittdienstleistern als für Finanzunternehmen kritisch“ (Art. 31(6) DORA) und die Guidelines zur „Festlegung der Höhe der von der federführenden Überwachungsbehörde bei kritischen IKT-Drittdienstleistern zu erhebenden Überwachungsgebühren und der Art und Weise der Entrichtung dieser Gebühren“ (Art. 43(2) DORA). Wie bereits erwähnt, ist das RTS 53 noch nicht final. Grundsätzlich unterscheidet DORA drei Stufen der Verbindlichkeit der IKT-Drittdienstleister (Abbildung 8):

1) Kritisch eingestufte IKT-Dienstleister,
2) IKT-Dienstleister von CIFs (kritische oder wichtige Funktionen) und
3) IKT-Dienstleister von allen IKT-Services.

**Drittanbieter von IKT-Dienstleistungen sind auf drei Ebenen von DORA betroffen**

| Option | | Thema | Alle IKT-Services | CIFs |
|---|---|---|---|---|
| 1 Klassifizierte kritische IKT-Drittdienstleiste (Artikel 31 (8) iii DORA) | ▪ **Direkte ESA-Aufsicht**<br>▪ **Viele strenge DORA-Pflichten** gelten, was die **Komplexität** der Vorschriften **steigert.** | 1. Anforderungen an die Form und Änderung vertraglicher Vereinbarungen | ✓ | erweitert |
| | | 2. Beschreibung des Services | ✓ | erweitert |
| | | 3. Beschreibung der Servicequalität | ✓ | erweitert |
| | | 4. Unterbeauftragung | ✗ | ja |
| | | 5. Standort | ✓ | ja |
| 2 Zulieferer von CIF | ▪ Es gelten **umfassende DORA-Verpflichtungen**, einschließlich einer detaillierten **Notfallplanung**, an das **Berichtswesen** und das **Melden von Vorfällen**.<br>▪ Die **vertraglichen Vereinbarungen** müssen diese erhöhten Verpflichtungen **widerspiegeln**, einschließlich klarer **Risikomanagement- und Compliance-Maßnahmen**. | 6. Datenschutz | ✓ | ja |
| | | 7. Datenzugang | ✓ | ja |
| | | 8. IKT-Vorfallmanagement | ✓ | ja |
| | | 9. Zusammenarbeit mit Aufsichtsbehörden | ✓ | ja |
| | | 10. Prüfungsrechte / kontinuierliche Überwachung | ✗ | ja |
| | | 11. Kündigungsrechte und -fristen | ✓ | erweitert |
| 3 Zulieferer von Nicht-CIF | ▪ **Reduzierte DORA-Anforderungen** zu erfüllen.<br>▪ Alle relevanten Verpflichtungen müssen in **Verträgen und SLAs** behandelt werden, einschließlich **Leistungs-, Sicherheits- und Überwachungsbestimmungen**.<br>▪ Auch bei reduziertem Umfang bleiben **grundlegendes Risikomanagement, Sicherheit und Überwachung** obligatorisch. | 12. Teilnahme an Fortbildungskursen des Finanzunternehmens | ✓ | ja |
| | | 13. Berichtspflichten | ✗ | ja |
| | | 14. Geschäftsfortführungspläne | ✗ | ja |
| | | 15. Spezifische IKT-Sicherheitsmaßnahmen | ✗ | ja |
| | | 16. Teilnahme an TLPT | ✗ | ja |
| | | 17. Ausstiegsstrategien | ✗ | ja |

*Abbildung 8: IKT-Drittdienstleistern stehen drei Stufen des DORA-Engagements zur Verfügung*

Kritisch eingestufte Dienstleister werden direkt von der federführenden Aufsichtsbehörde überwacht. Welche dies sein werden wird von den ESAs nach dem Erhalt der Informationsregister im April 2025 untersucht und festgestellt. Die IKT-DDL werden bis Juli 2025 über ihre Einstufung als kritisch informiert. Mit dieser Benachrichtigung beginnt eine sechswöchige Frist, innerhalb derer die IKT-Drittdienstleister mit einer begründeten Erklärung und entsprechenden[10] Belegen Einspruch gegen die Bewertung einlegen können. Allerdings geht auch die BaFin davon aus, dass man die Einstufung eher als Qualitätssiegel in der Zukunft wahrnehmen könnte.[11]

Dienstleister für CIFs haben weitaus mehr und detailliertere Anforderungen zu erfüllen als Dienstleister von Nicht-CIFs. Beispiele für weitere Anforderungen sind Inspektionsrechte und eine kontinuierliche Überwachung durch das auslagernde Finanzunternehmen oder auch Berichtspflichten, Geschäftsfortführungspläne sowie die Unterstützung bei einer Exit-Strategie.

## 6 TLPT – Ein Vergleich DORA zu TIBER-EU

Im Januar 2025 hat die EZB ihr TLPT-Schema TIBER-EU[12] in einer aktualisierten Version veröffentlicht. Das TLPT-Schema nach DORA besteht aus dem Kapitel IV „Testen der digitalen Resilienz“ mit den Artikeln 24 bis 27 DORA und dem RTS 29 aus dem Juli 2024. Beide Schemas sollten in wesentlichen Inhalten gleich sein, da sowohl DORA im RTS 29 angekündigt hatte, dass das TIBER-EU Framework an die Regelungen der DORA angeglichen wird, als auch TIBER-EU im September 2024 ausgeführt hatte, dass DORA eine Übereinstimmung der technischen Regulierungsstandards für TLPT in Übereinstimmung mit dem TIBER-EU-Rahmen verlangt.

**Vergleich der EU-Rahmenbedingungen für bedrohungsbasierte Penetrationstests (TLPT)**

**Stakeholder-Rollen**

| TIBER-EU | DORA | Ähnlichkeit |
|---|---|---|
| TIBER Cyber Team & Test Manager | TLPT Cyber Team (TCT) & Test Manager | Gleich |
| Control Team & Control Team Lead | Control Team & Control Team Lead | |
| Blue Team | Blue Team | |
| TIP[8] | TIP[9] | |
| Red Team Tester | Red Team | |

**Zeitaufwand**

| TIBER-EU | DORA | Ähnlichkeit |
|---|---|---|
| 40 bis 63 Wochen | 38 bis 40 Wochen | TIBER-EU erlaubt deutlich längere Übergangs- und Feedbackphasen |

**Kontaktpunkte mit Aufsicht**

| TIBER-EU | DORA | Ähnlichkeit |
|---|---|---|
| 10 Kontaktpunkte | 12 Kontaktpunkte | Ähnlich |

**Dokumente**

| TIBER-EU | DORA | Ähnlichkeit |
|---|---|---|
| 12, z.B.: | 11, z.B.: | Ähnlich |
| Targeted Threat Intelligence Report | Threat Intelligence Report | Übersicht Bedroh-ungsszenarien |
| Red Team Test Plan | Red Team Test Plan | Testmethodik & Ressourcen-management |
| Scoping-Dokument | Scope Specification Dokument | Klar definierter Testumfang & Leitlinien |

**Phasen**

| TIBER-EU | DORA | Ähnlichkeit |
|---|---|---|
| 1. Einführung und Implementierung | 1. Preparation | Ähnlich |
| 2. Vorbereitungs-phase | 2. Testing Phase: Threat Intelligence | Starke inhaltliche Abweichung |
| 3. Threat Intelligence & red Red Team Test | 3. Testing Phase: Red Team Test | Große inhaltliche Unterschiede |
| 4. Abschluss-phase | 4. Abschluss-phase | Ähnlich |

| | DORA | DORA + TIBER-EU | TIBER-EU |
|---|---|---|---|
| Interne Tester | ▪ Signifikante Kreditinstitute dürfen keine internen Tester verwenden (Artikel 26(8) DORA) | ▪ In beiden Schemes nur mit Genehmigung der Aufsichtsbehörde (Artikel 27(2) lit. a DORA, Kapitel 3.6.3 TIBER-EU)<br>▪ Spätestens nach zwei Tests mit internen Testern müssen externe Tester verwendet werden (Artikel 26(8) lit. c DORA, Kapitel 3.6.3 TIBER-EU) | ▪ Tester eines internen IKT-Dienstleisters gelten bei beiden Schemas als interne Tester (Artikel 13 Nr. 3 RTS 29 DORA, Kapitel 3.6 TIBER-EU) |
| TIP | ▪ Bei DORA muss der TIP extern sein, wenn interne Tester verwendet werden (Artikel 27(2) lit.c DORA). | | ▪ In TIBER-EU ist die Verwendung eines externen TIP obligatorisch (Kapitel 3.6). |
| Interne Tester + TIP | ▪ Bei beiden Schemes dürfen TIP und externe Tester vom selben Unternehmen sein (Artikel 5(2(ev.) und 2(f)v.) RTS 29 DORA, Table 1/Table2 TIBER-EU GSPP) | | |

1: TIBER: Threat Intelligence-based Ethical Red-Teaming I 2: DORA: Digital Operational Resilience Act

*Abbildung 9: TLPT nach DORA und TIBER-EU – Gleichanteile, Ähnlichkeiten und Unterschiede*

Abbildung 9 illustriert die Übereinstimmung beider Schemas in den Metathemen Stakeholder, Zeitbedarfe, Kontaktpunkte zur Aufsicht, Dokumente und Phasen. Einzig der Zeitbedarf zeigt eine deutliche Abweichung bei den zwei Schemas: 38 bis 40 Wochen bei DORA zu 40 bis 63 Wochen bei TIBER-EU. Diese Angaben basieren zwar auf der Summe der Zeitangaben in den beschreibenden Texten, jedoch sind die Genehmigungsbedarfe durch die Aufsichtsbehörden und ihre weiteren Mitwirkungspflichten nicht inkludiert, da sie nicht abschätzbar sind. Zudem sind parallel ausführbare Aktivitäten bei beiden Schemas seriell beschrieben. In der Ausführungspraxis dürften sich nach Ansicht der Autoren die Zeitdauern der zwei Schemas kaum signifikant unterscheiden.

TIBER-EU wurde bisher in 16 europäischen Ländern angewendet, in einigen freiwillig und in einigen obligatorisch für Kreditinstitute. Die DORA ist obligatorisch in allen Mitgliedsländern der EU. Zusätzlich wirkt sie über das Management von Drittparteienrisiken über die EU hinaus, indem zum Beispiel nicht-europäische IKT-Drittdienstleister ein europäisches Finanzunternehmen bei der Durchführung eines TLPT unterstützen müssen.

Während TIBER-EU für Banken entwickelt wurde, gilt DORA für 20 Arten von Finanzunternehmen und für IKT-Drittdienstleister. TIBER-EU wiederum ist grundsätzlich offen für die Anwendung in anderen Sektoren außerhalb des Finanzsektors. Technisch und organisatorisch ist auch das TLPT-Schema nach DORA für die Nutzung in anderen Sektoren geeignet, allerdings ist DORA nur für den Finanzsektor anzuwenden.

TIBER-EU liefert mehr Informationsmaterial (siehe Quellen) und ist vornehmlich in Prosa anstatt in kleinen abgegrenzten Topics in Form von Artikeln verfasst. Dadurch sind die Details in der DORA und im RTS 29 schneller zu erfassen. Das kann vor allem für Organisationen, die erst mit der DORA über TLPT nachdenken müssen, ein Vorteil sein.

Summa summarum wurden sich mit der EZB und den ESAs zwei Europäische Institutionen nicht einig, sodass jetzt zwei Schemas für TLPT im Finanzsektor nebeneinander existieren. Rechtlich verbindlich ist einzig TLPT nach DORA. Besser wäre ein einziges Schema. Zwar betonen beide Institutionen, dass die Schemas integriert sind, faktisch gibt es aber zwei. Das kann Marktteilnehmer, vor allem solche, die bisher kein TLPT durchzuführen hatten, irritieren. Positiv betrachtet stehen den Marktteilnehmern zusammengenommen mit den zwei Schemas umfangreiche Materialien zur Umsetzung von TLPT zur Verfügung.

TLPT wird zum Mindest-Standard – es ist besser sich früh damit auseinanderzusetzen.

In der Praxis dürfte sich eine zweigeteilte Lage einstellen:

- Banken, die bereits TLPT nach TIBER-EU durchgeführt haben, werden dies weiterhin tun, und Kleinigkeiten in den Dokumenten, bei Bezeichnungen und im zeitlichen Ablauf anpassen, um der DORA zu genügen.
- Finanzunternehmen, für die TLPT gänzlich neu ist, werden zuerst dem Gesetz und somit der DORA genügen und ihr TLPT-Schema nach dem RTS 29 aufbauen.

In Deutschland spiegelt sich die Zweiteilung in Europa mit EZB und den ESAs seit langem in den bekannten „44er-Prüfungen“ wider: Die BaFin als Überwachungsbehörde ist für das Audit verantwortlich, während die Bundesbank die Prüfer stellt. Bei signifikanten Instituten werden die Prüfer der Bundesbank durch Prüfer der EZB unterstützt. Das dürfte auch bei den DORA-Prüfungen der Fall sein: Die BaFin als Verantwortliche wird sich Prüfer der Bundesbank bedienen. Es muss zudem abgewartet werden, wie das finale RTS 29 aussehen wird. Derzeit steht nur ein „Final Report“ vom 17. Juli 2024 zur Verfügung.

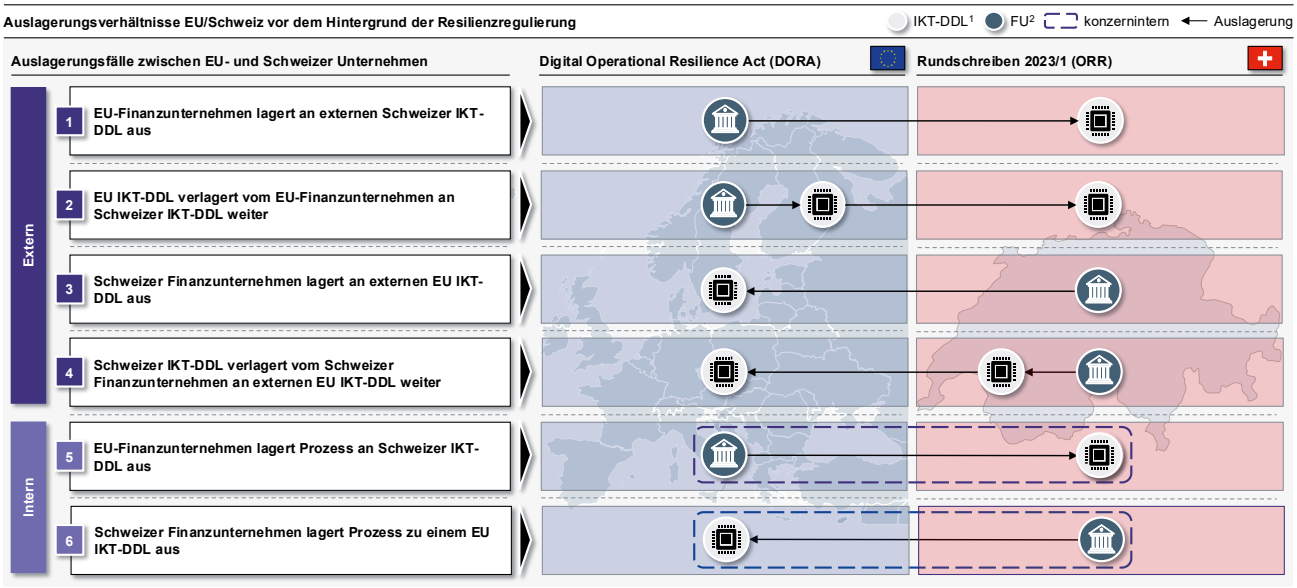
## 7 DORA hinter dem EU-Horizont

Der Einkauf von Expertise und Softwarelösungen über die EU hinaus sind heute Standardpraxis. Neuerungen rund um die Kontrolle und Überwachung dessen stellen Finanzunternehmen und IKT-DDL vor Herausforderungen bei gleichzeitiger Sicherstellung der Compliance.

### 7.1 Die Schweiz sorgt für Kompatibilität zur DORA

Die Schweiz verfügt mit dem Anfang 2024 in Kraft getretenen „Rundschreiben 2023/1 – Operationelle Risiken und Resilienz – Banken“[13] über eine Adaptation zur DORA. Das Themenspektrum umfasst mit Ausnahme des Testens der operationellen Resilienz das der DORA. Während die DORA detaillierte Vorgaben an die Aufbau- und Ablauforganisation

formuliert, bleibt das Schweizer Pendant grundsätzlich allgemein. Zum Verständnis ein Vergleich aus der Standardisierung der Informationssicherheit: das Schweizer Rundschreiben formuliert lediglich Anforderungen und bleibt so auf der groben Ebene des ISO-Standards 27001, während die DORA durch kleinteilige Formulierung von Anforderungen im Stil und Umfang des ISO-Standards 27002 agiert. In der Praxis sind sechs Betriebskonstellationen zwischen EU und Schweiz von Relevanz (Abbildung 10).




Quelle: GRM | 1: IKT-Drittdienstleister | 2: Finanzunternehmen

*Abbildung 10: Auslagerungsverhältnisse zwischen der EU und der Schweiz*

Im ersten Fall wird das EU-Finanzunternehmen beim Auslagerungsunternehmen aus der Schweiz auf DORA-Konformität bestehen. Hier kommt es für den Schweizer IKT-DDL auf die individuellen Abweichungen zwischen dem Ist-Stand seiner IKT und dem Soll des Rundschreibens an. Im zweiten Fall verbleibt das EU-Finanzunternehmen verantwortlich für die gesamte Auslagerungskette, sodass es auch vom Unterauslagerungsnehmer aus der Schweiz Konformität zur DORA verlangen muss. Im dritten Fall wird das Schweizer Finanzunternehmen den DORA-konformen IKT-DDL aus der EU akzeptieren, da die Schweiz über eine an DORA angelehnte Regulierung verfügt. Im vierten Fall wird das auslagernde Schweizer Finanzunternehmen EU IKT-DDL kontrahieren können, da diese mit der DORA die Schweizer Anforderungen (über-)erfüllen. Das gilt auch für den sechsten Fall, bei dem im internen Auslagerungsverhältnis kein weiterer IKT-DDL zwischengeschaltet ist. Der fünfte Fall ist die konzerninterne Variante des ersten Falls: der Schweizer IKT-DDL muss DORA-konform sein.

Schweizer IKT-DDL können EU-Finanzunternehmen aus der Schweiz heraus bedienen. Wenn die EU ein Schweizer IKT-DDL als kritisch einstuft, muss das Unternehmen innerhalb von zwölf Monaten eine Tochtergesellschaft in der EU gründen. Wie im Datenschutz (siehe unser White Paper zum Schweizer Datenschutzgesetz) erreicht die Schweiz auch zur operationellen Resilienz Äquivalenz zur EU mit deutlich geringerem Aufwand für den Schweizer Finanzsektor.

## 7.2 Aus der EU in die EU – Die Besonderheit der Brexit-Banken

In der EU gelegene Zweigstellen von Brexit-Banken verfügen über keinen Europäischen Pass und können regulierte Tätigkeiten nur ausüben, wenn eine entsprechende Erlaubnis der Europäischen Zentralbank (EZB) und der nationalen Behörde vorliegt. Umgekehrt bedeutet dies, dass Zweigstellen in Drittländern keine kritischen Funktionen übernehmen und keine Dienstleistungen für Kunden in der EU erbringen sollten[14]. Sobald ein Finanzprodukt in einem EU-Mitgliedstaat zugelassen ist, kann es in der gesamten Union vertrieben werden.

Nutzen Finanzinstitute gruppenweite Infrastruktur, Expertise und Strukturen aus einem Drittland, müssen alle IKT-relevanten Risiken unabhängig und auf lokaler Ebene gesteuert und überwacht werden. Im Falle eines Audits bedeutet dies, dass Anfragen sofort und eigenständig beantwortet und entsprechende Auskünfte erteilt werden[15].

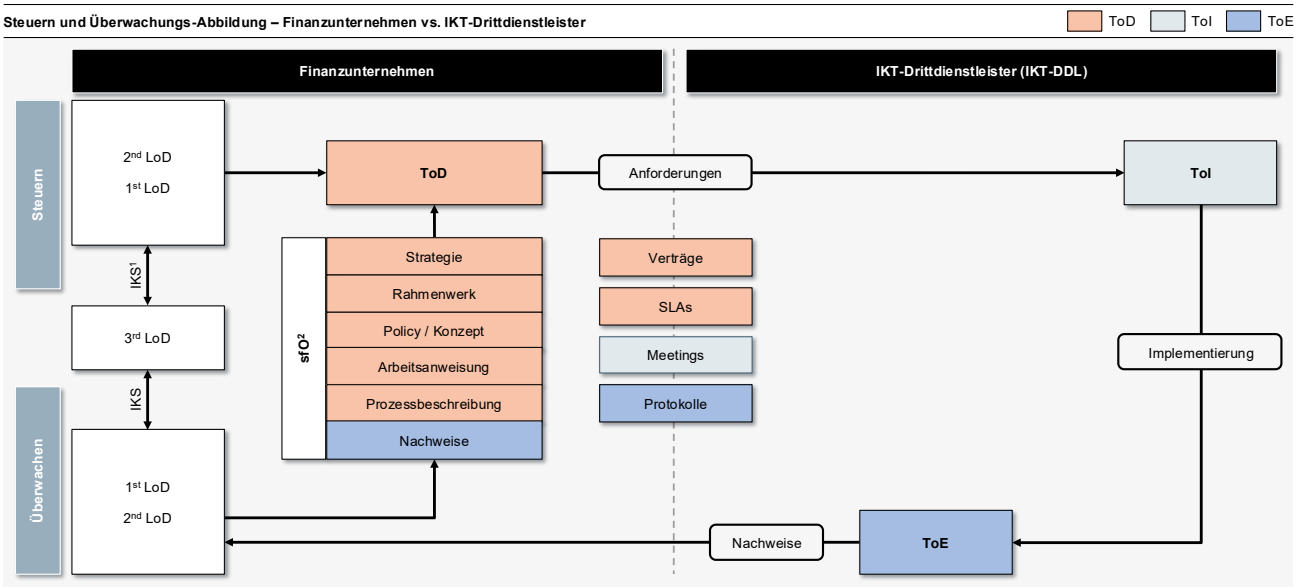



*Abbildung 11: Steuern und Überwachen im Verhältnis Finanzunternehmen zu IKT-Drittdienstleister*

Grundsätzlich müssen EU-Banken eigene Kontrollfunktionen vorhalten, die sowohl quantitativ als auch qualitativ angemessen besetzt sind. Eine vollständige Auslagerung dieser Funktionen, beispielsweise an die Unternehmenszentrale in London, ist daher nicht zulässig[16]. Ein robustes Risikocontrolling befähigt die Leitungsebene, diese Aufgaben bei Auslagerungen (innerhalb oder außerhalb der Gruppe) im Sinne der aufsichtlichen Anforderungen zu erfüllen (Abbildung 11). Außerdem trägt es durch zusätzliche Notfallverfahren inklusive der regelmäßigen Wirksamkeitsprüfung zur operativen Unabhängigkeit des Aufsichtsobjektes bei[17]. Dies erstreckt sich ebenfalls über die Auslagerung[18].

In der Praxis bei der Nutzung verschiedener Strukturen einer Brexit-Mutterbank bedeutet dies für das Finanzinstitut innerhalb des EWR, dass es keine Abkürzungen gibt. Die Finanzaufsicht lässt einen einfachen Verweis auf Gruppenrichtlinien und genutzte Funktionen, die sich auf das Steuern und Überwachen beziehen, nicht zu. Die Bank muss eine Übersicht über alle Auslagerungen bzw. von der Mutterbank genutzte Strukturen verfügen und diese selbstständig steuern und überwachen.

Komplexer wird es, wenn die gesamte Infrastruktur der Mutterbank genutzt wird und es damit eine wesentliche Auslagerung gibt, die wiederum Unterauftragnehmer mit direkter Auslagerungsbeziehung unterhält. Eine Übersicht der Dienstleistungen, die das Finanzunternehmen ebenfalls innerhalb des EWR nutzt, muss ihr vorliegen. Der Leitungsebene muss mindestens einmal jährlich der Bericht zu wesentlichen Auslagerungen vorgelegt werden (§ 25b KWG). Ein formelles Mitteilungsverfahren manifestiert sich ebenfalls in den externen Prüfberichten der Jahresabschlüsse nach §9 Absatz 3 sowie Anhang 4 der Prüfberichtsverordnung (PrüfBV).

Für Finanzinstitute, die in der EU als Teil einer Drittlandsgruppe ohne EU-Mutterunternehmen tätig sind, schreibt die DORA vor, dass das Informationsregister auf Einzelunternehmensebene einzureichen ist. Das bedeutet, dass dort nur das berichtende Finanzunternehmen selbst aufgeführt werden muss, ohne dass eine Verpflichtung besteht, andere Konzerngesellschaften mit Sitz in anderen EU-Mitgliedstaaten oder außerhalb der EU anzugeben, es sei denn, es handelt sich um direkte Tochtergesellschaften und deren Zweigstellen. Wenn jedoch eines dieser Drittlands- oder EU-inneren Konzerngesellschaften IKT-Dienstleistungen für das berichtende Unternehmen erbringt, muss es als konzerninterner Dienstleister angegeben und gemeldet werden, während die Berichterstattung darüber hinaus bis auf den ersten externen Dienstleister gehen muss[19].

Zusammengefasst heißt dies, dass man zwischen einer konsolidierten aufsichtsrechtlichen Gruppe (nur EU) und der Gruppe als Konzern (mit Mutterkonzern außerhalb der EU) unterscheiden muss. Dadurch wird die Transparenz der internen IKT-Abhängigkeiten gewährleistet und gleichzeitig eine Übererfassung nicht verbundener Konzernstrukturen vermieden.

## 8 Fazit

DORA ist ein sinnhaftes, zielführendes und angemessenes Gesetz. Das trifft nicht auf alle großen Regulierungsvorhaben der EU zu. Sinnhaft da der Finanzsektor auf IKT beruht und insgesamt als kritisch für die Versorgung von Wirtschaft, Staat und Bürger eingestuft ist. DORA ist auch zielführend, da die formulierten Anforderungen einzeln und gemeinsam dem Ziel der operationellen Resilienz dienen. DORA ist nicht zuletzt auch angemessen ausgestaltet. Zwar sind einzelne Anforderungen sehr detailliert und stellen sich damit für einige Entitäten als herausfordernd dar. Jedoch kann die Gesamtkomposition der Breiten- und Tiefengestaltung als effektiv und effizient bezeichnet werden.

In Deutschland werden neben den bereits aus XAIT/MaX beaufsichtigten ca. 1.200 weitere Finanzunternehmen erstmals in ihrer IT beaufsichtigt. Zudem müssen sich die ca. 3.750 deutschen IKT-Drittdienstleister zur DORA verhalten, nicht nur die als kritisch eingestuften, sondern auch alle anderen, denn ohne das Siegel der Bankenaufsicht „kritisch im Sinne der DORA“ werden diese einen Nachteil im Wettbewerb erfahren.

Der neu geforderte IKT-Risikomanagementrahmen kann als Untersystem des ohnehin vorhandenen allgemeinen Risikomanagementsystems aufgebaut und betrieben werden. Der Aufbau einer gänzlich neuen, womöglich parallelen Struktur speziell für IKT-Risiken ist nicht notwendig. Stattdessen kann die vorhandene Risiko-Governance aus schriftlich fixierter Ordnung der IT-Ausstattung, den zugeordneten Gremien und dem Risiko- und Sicherheits-Personal um die IKT-Bedarfe erweitert werden.

Mit dem Wegfall der Wesentlichkeitsbeurteilung nach BAIT muss ein separates Beurteilungsschema für die Identifizierung von kritischen oder wichtigen Funktionen betrieben werden. Zudem ist die Neuverhandlung aller Verträge notwendig. Ist diese Phase erstmal abgeschlossen, was nach Marktsignalen erst im kommenden Jahr der Fall sein wird, sollte das Kapitel Outsourcing in ruhigere Fahrwasser geraten. Bis dahin okkupiert das IKT-Drittparteienmanagement den größten Ressourcenanteil in allen DORA-Umsetzungsprojekten.

Auch das Vorfallmanagement wird mit DORA auf eine neue Grundlage gestellt mit dedizierten Schwellwerten und Fristen. Das Melderegime nach PSD2 für schwerwiegende Betriebs- und Sicherheitsvorfälle bei Zahlungsdienstleistern wurde mit der DORA folgerichtig abgelöst. Insgesamt ist das Meldewesen klar strukturiert, verbindlich und damit gelungen. Ab Q3 2025 wird interessant zu beobachten sein, wie sich die nicht als kritisch eingestuften IKT-Drittdienstleister nach dem Entscheid der ESA positionieren werden. Die Nicht-Einstufung könnte sich als Malus am Markt erweisen.

Mit der Anpassung von TIBER-EU an die DORA hat es der Europäische Regulierer leider versäumt für Klarheit zu sorgen, denn diese „Parallel-Aktion“ stiftet höchstens Verwirrung anstatt der beabsichtigten Resilienz. Die Konzentration auf TLPT nach DORA ist aber der sichere Weg. Die Schweiz erweist sich wieder als smarter als die EU: wie schon beim Schweizer Datenschutzgesetz kann der Schweizer Finanzmarkt von einer Regulierung der Resilienz mit Augenmaß profitieren, bei geringeren Aufwänden aber mit Akzeptanz durch die EU. Nicht zuletzt das Beispiel Brexit-Banken mit ihren oft weltweit verteilten Governance zeigt die überragende Stellung einer ausgereiften ToX-3LoD-Systematik.

## Quellenverzeichnis


1. BaFin. (2024). Bekanntmachung zur Citibank N.A. in New York, Filiale Frankfurt am Main. Bonn: Bundesanstalt für Finanzdienstleistungsaufsicht.
2. BaFin. (2025). Deutsche Bank AG: BaFin setzt Geldbußen fest. Bonn: Bundesanstalt für Finanzdienstleistungsaufsicht.
3. BaFin. (2025). SECB Swiss Euro Clearing Bank GmbH: BaFin ordnet Sicherstellung der ordnungsgemäßen Geschäftsorganisation und zusätzliche Eigenmittelanforderungen an. Bonn: Bundesanstalt für Finanzdienstleistungsaufsicht.
4. BaFin. (o.J.). Banken, Finanzdienstleister und Wertpapierinstitute. Bonn: Bundesanstalt für Finanzdienstleistungsaufsicht.
5. BaFin. (2024). DORA. Bonn: Bundesanstalt für Finanzdienstleistungsaufsicht.
6. Europäische Bankenaufsichtsbehörde. (2023). ESAs Report on the Landscape of ICT Third-Party Providers in the EU. Paris: EBA.
7. National Institute of Standards and Technology. (o.J.). Cybersecurity Framework 2.0. Gaithersburg, MD: NIST.
8. EIOPA. (o.J.). ITS zum Informationsregister. Frankfurt: Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung.
9. Europäische Bankenaufsichtsbehörde. (o.J.). Technische Standards zur Unterauftragsvergabe im Rahmen von DORA. Paris: EBA.
10. Europäische Bankenaufsichtsbehörde. (o.J.). Zeitplan zur Erhebung von Informationen zur Benennung kritischer IKT-Drittanbieter. Paris: EBA.
11. BaFin. (2025). Konzentrationsrisiken bei Auslagerungen im Rahmen von DORA. Bonn: Bundesanstalt für Finanzdienstleistungsaufsicht.
12. Europäische Zentralbank. (o.J.). TIBER-EU Rahmenwerk. Frankfurt: Europäische Zentralbank.
13. FINMA. (2023). Operationelle Risiken und Resilienz – Banken. Bern: Eidgenössische Finanzmarktaufsicht.
14. Bundesministerium der Justiz. (2024). Kreditwesengesetz (KWG), §32(1). Berlin: Bundesministerium der Justiz.
15. Europäische Zentralbank. (2024). Relocation in den Euroraum. Frankfurt: Europäische Zentralbank.
16. Bundesministerium der Justiz. (2024). Sanierungs- und Abwicklungsgesetz (SAG). Berlin: Bundesministerium der Justiz.
17. BaFin. (2017). Brexit-Workshop: Auswirkungen auf Banken und Finanzdienstleister. Bonn: Bundesanstalt für Finanzdienstleistungsaufsicht.
18. BaFin. (2024). Mindestanforderungen an das Risikomanagement (MaRisk) AT9: Steuerung von Auslagerungsmaßnahmen. Bonn: Bundesanstalt für Finanzdienstleistungsaufsicht.
19. Europäische Aufsichtsbehörden. (2025). FAQ: Meldung von Informationsregistern nach DORA. Paris: ESA.

## Autoren

**Julius Düwel** | Managing Director

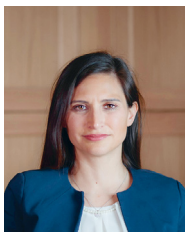
Julius ist Experte für besondere regulatorische Situationen und die Begleitung finanzaufsichtlicher Sonderprüfungen. Er unterstützt Klienten in allen Phasen solcher Prüfungen und bringt dabei seine umfassende Erfahrung im Umgang mit unterschiedlichen Stakeholdern auf Unternehmens- und Aufsichtsseite ein. Ein besonderer Schwerpunkt seiner Arbeit liegt auf der Bewertung, Steuerung und Kommunikation von regulatorischen und operationellen Risiken im Prüfungsumfeld.

**Mail:** jdu@globalregulation.com

**Dr. Waldemar Grudzien** | Managing Director

Waldemar ist Experte für finanzaufsichtliche Prüfungen, Informationssicherheit und Datenschutz. Er unterstützt Klienten in allen Phasen bei aufsichtlichen Prüfungen sowie bei der Einhaltung von Informationssicherheits- und Datenschutzanforderungen. Als promovierter Elektroingenieur und studierter Wirtschafts-wissenschaftler war er bei einem Verband der Kreditwirtschaft als Experte für Sicherheit im Retail- und Online-Banking tätig.

**Mail:** wgr@globalregulation.com



**Nadine Hofmann** | Director

Nadine ist Expertin für Managementsysteme der Informationssicherheit und des Datenschutzes nach den ISO-Standards. Dies beinhaltet die Implementierung von Maßnahmen für Finanzinstitute über die Definition von Anforderungen und Prozessen bis hin zur Vorbereitung von Audits, als auch der Migration von Prüfungsergebnissen. Sie schloss das Studium zu Luft- und Raumfahrttechnik an der TU Braunschweig und TU Dresden ab.

**Mail:** nho@globalregulation.com

**Farahnoz Mirboboeva** | Manager

Farahnoz‘ Fachwissen erstreckt sich auf die Implementierung von ISMS, Projektmanagement und Strategieentwicklung. Sie hat u.a. Projekte zu Kernbankensystemen, zu Prüfungen und zu Entwicklung von Geschäfts- und IT-Strategien geleitet. Darüber hinaus unterstützt Farahnoz Kunden in Compliance-Projekten wie DORA und speziell bei der Entwicklung und Implementierung robuster Prozesse für das Incident Management.

**Mail:** fmi@globalregulation.com

## Über Global Regulation Management AG

GRM hebelt Regulierung. Unsere Mission ist der Aufbau regelkonformer Unternehmensstrukturen für global agierende Organisationen. Dabei setzen wir auf ein tiefes Verständnis von Geschäftsprozessen, den rechtlichen Anforderungen in Zielmärkten sowie den gezielten Einsatz moderner Softwarelösungen. Die enge Verzahnung von Geschäftsentwicklung, Risikomanagement und regulatorischen Vorgaben in einer globalisierten Wirtschaftswelt stehen im Mittelpunkt. Das Ergebnis unserer Arbeit sind sichere, rechtskonforme und international operierende Unternehmensstrukturen.

## Copyright-Anspruch

## Kontakt

Global Regulation Management AG
Baarerstrasse 52
6300 Zug
Schweiz

info@globalregulation.com
**https://globalregulation.com**