TaylorWessing

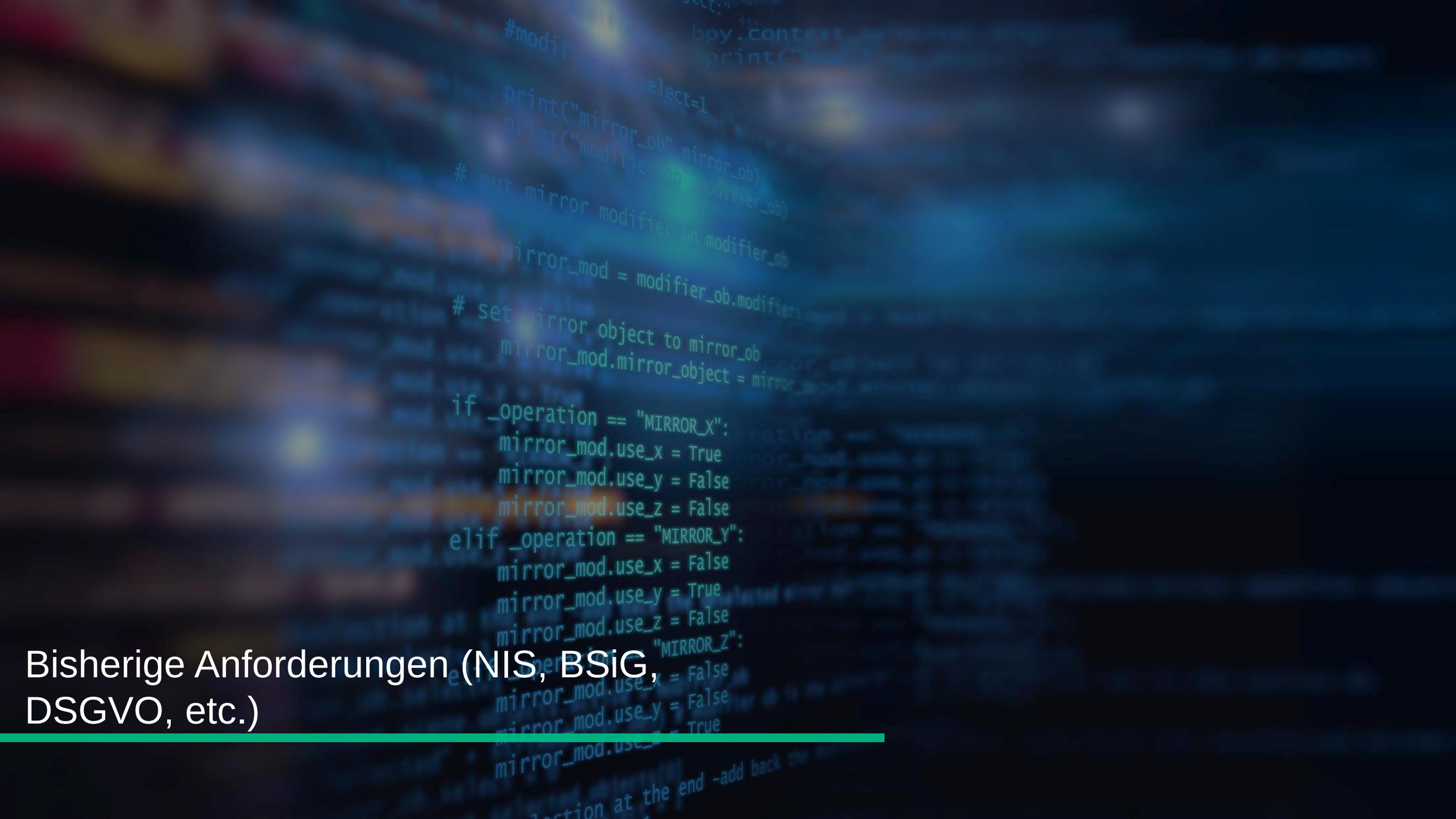
Exploring DORA #2: Das big Picture des IT-Sicherheitsrechts für die Finanzindustrie

Thomas Kahl, Dr. Verena Ritter-Döring

20.06.2023

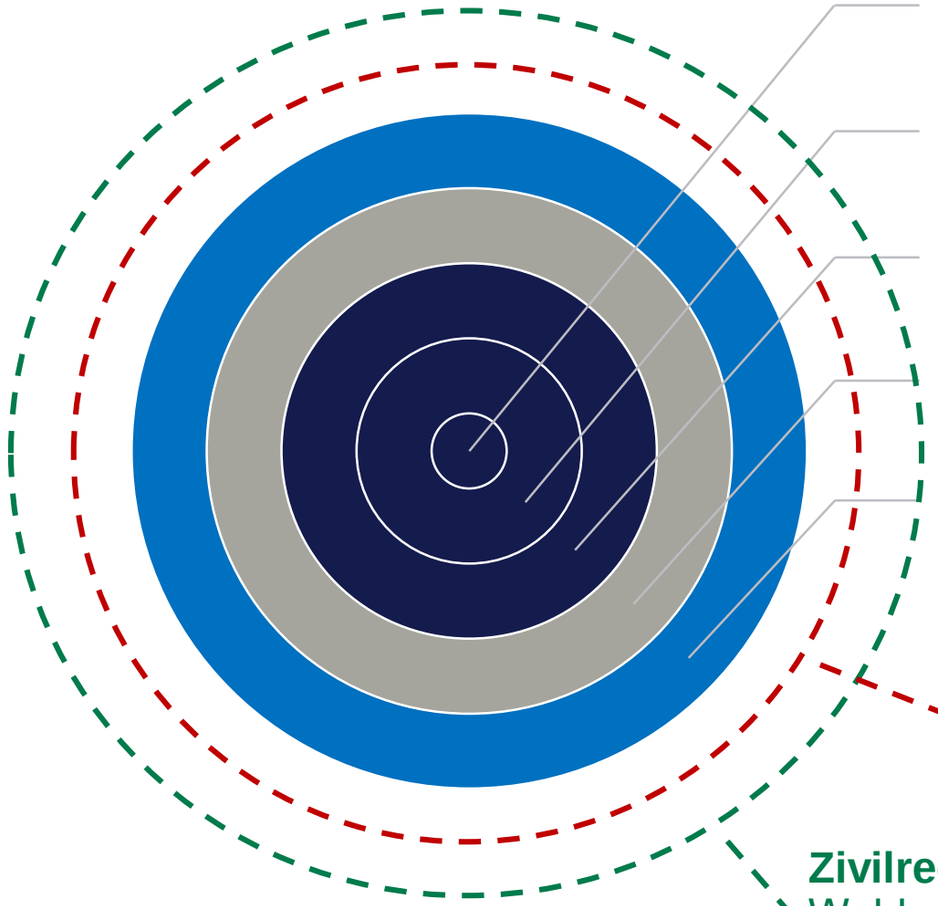
Agenda

1	Bisherige Anforderungen (NIS, BSiG, DSGVO, etc.)	3
2	DORA und die Abgrenzung zu sonstigen Regelwerken im Aufsichtsrecht	6
3	DORA und die Verwaltungspraxis der BaFin (BAIT, ZAIT, KAIT)	8



Bisherige Anforderungen (NIS, BSiG, DSGVO, etc.)

IT-Sicherheitsrecht - “*Was bisher geschah …*”



Branchenstandards, Zertifizierungen, Initiativen (z.B. ISO-Normen wie 2700x, BSI IT-Grundschutz 200-1 bis 4, B3S u.a. für Versicherungen oder Cash-Netzbetreiber, Teletrust / ENISA „Stand d. Technik“ Guidelines)

Branchenspezifische Guidelines (konkretisieren gesetzl. Anforderungen aus KWG / BSIG, z.B. BAIT/VAIT-Novelle (2021); EBA Guidelines ICT & Security Risk Management (2019) und Outsourcing-Arrangements; MARisk 2019 / MaGO (=> Verw.-Vorschriften)

Branchenspezifische Gesetzgebung wie KWG und BSiG (IT-Sicherheitsgesetz 2.0 + KRITIS-VOen (Stand `23) in Umsetzung der NIS-RL => materielle Gesetze; Zukunft: NIS2-UmsG + „Dachgesetz“)

DS-GVO und nationales DS-Recht (pb Daten)

Europäischer Rechtsrahmen für Cyber-Sicherheit (**NIS 2** und EU Critical Entities Resilience Directive (**CER**; entspricht weitestgehend Anhang I NIS 2 / KRITIS Sektoren = auch Banken)

Allgemeine Gesellschaftsrechtliche Anforderungen (u.a. 91 AktG) und **Compliance-Anforderungen** (u.a. CMS einschl. ISMS; § 43 GmbH, §§ 93, 116 AktG)

Zivilrechtliche Pflichten / Haftung (Schutz- und Wohlverhaltenspflichten, zuletzt auch durch „digitales Kaufrecht“ und Gewährleistung)

„Flickenteppich“ IT-Sicherheitsgesetzgebung für Finanzindustrie

EU- Cybersicherheitsstrategie

Cyber Security Act (CSA) [Zertifizierung IKT-Produkte]

Cyber Resilience Act (CRA) [IT-Sicherheit HW, SW, Services]

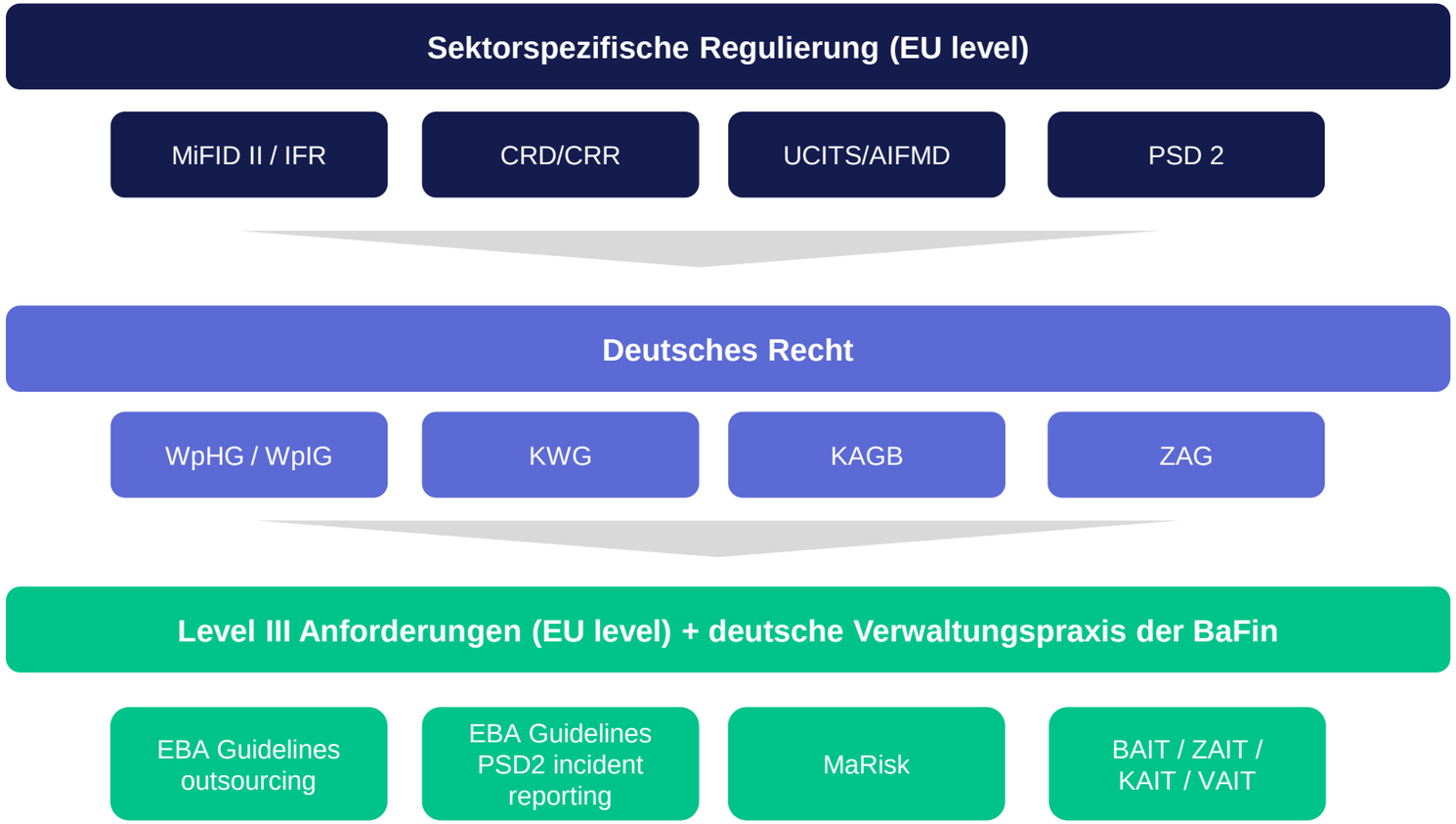
The Network and Information Security Directive (NIS-2)

Digital Operational Resilience Act (DORA)

Resilience of Critical Entities Directive (RCE)

DORA und die Abgrenzung zu sonstigen Regelwerken im Aufsichtsrecht

IT-Regulierung im geltenden Aufsichtsrecht



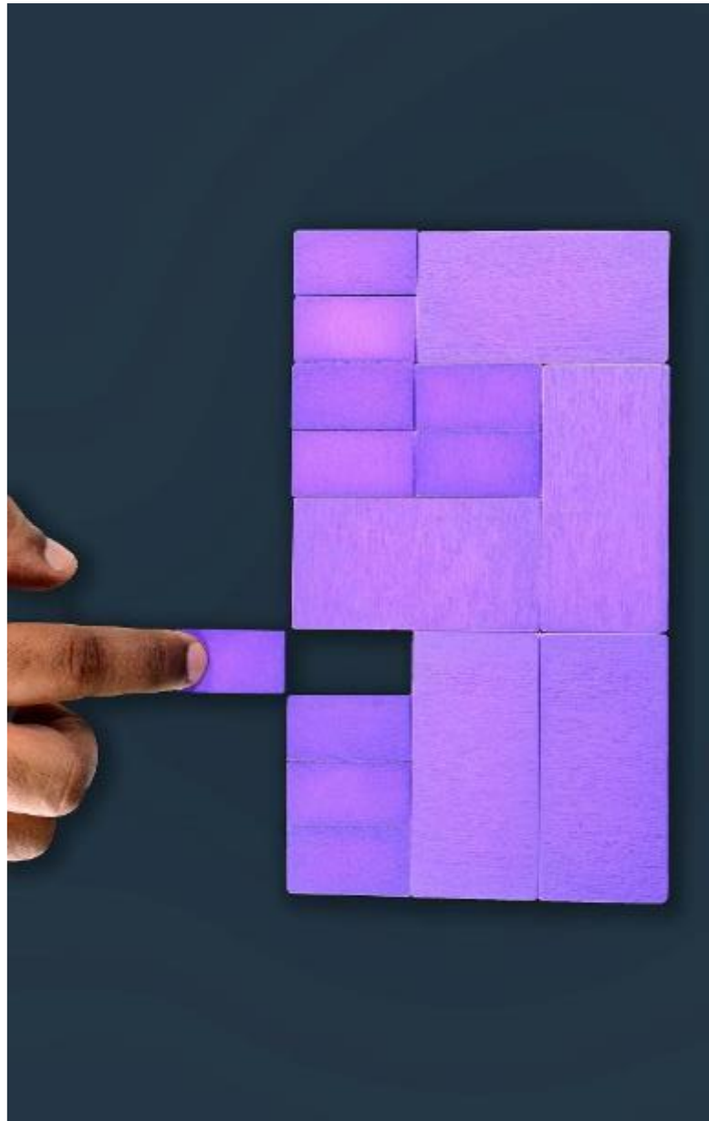
DORA

Digital Operational Resilience Act (DORA) - Überblick

- Teil des **EU Digital Finance Packages** vom 24. September 2020
- Es gibt eine Verordnung und eine Richtlinie.
- Ziel ist die **Harmonisierung** der wichtigsten Anforderungen an die digitale operationale Resilienz für alle Finanzunternehmen in der EU.

- Für Deutschland gilt, dass ein großer Teil der DORA-Anforderungen im Wesentlichen bereits aus bestehenden Regulierungen und der aufsichtlichen Verwaltungspraxis wie den MaRisk i.V.m. den BAIT und den EBA Guidelines on Outsourcing bekannt sind. Mit DORA werden diese aber konkretisiert und um neue, zusätzliche Aspekte ergänzt.
- **Compliance mit DORA ≠ Compliance mit BAIT/ZAIT/KAIT**
- Schaffung eines einheitlichen und sektorübergreifenden Aufsichtsrahmens für IKT-Risiken und IKT-Drittparteienrisiken

- Trat in Kraft am **16. January 2023**
- Anwendbar ab **17. January 2025**
- Der Umsetzungsbedarf sollte nicht unterschätzt werden; wir empfehlen eine zeitige Analyse der neuen Anforderungen und eine Gap-Analyse zum status quo.



DORA auf einen Blick

IKT-Risikomanagement	Art. 5 - 16
Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle	Art. 17 - 23
Testen der digitalen operationalen Resilienz	Art. 24 - 27
Management des IKT-Drittparteienrisikos	Art. 28 - 44
Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen	Art. 45 - 56

DORA und die Verwaltungspraxis der BaFin (BAIT, ZAIT, KAIT)

Verwaltungspraxis der BaFin

BAIT: Bankaufsichtlichen Anforderungen an die IT
ZAIT: Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten
KAIT: Kapitalverwaltungsaufsichtlichen Anforderungen an die IT
VAIT: Versicherungsaufsichtliche Anforderungen an die IT

+ MaRisk / KaMaRisk / EBA Guidelines zu PSD2 und zu Outsourcing

- Die Vorgaben in DORA sind nun auf Gesetzesebene verankert (Europäische Verordnung) und nicht mehr nur in Rundschreiben (Verwaltungsvorschriften) der BaFin.
- Da DORA im Vergleich zur BAIT, VAIT und KAIT konkretere Vorgaben enthält, werden derzeit bestehende Ermessens-spielräume die Finanzmarktakteure erheblich reduziert.
- Aber auch DORA bestätigt den Proportionalitätsgrundsatz. Daher kein *One fits all*.

IKT-Risikomanagementrahmen

1. **Identifizieren, Klassifizieren und Kommunizieren** der ICT-Risiken (inkl. jährlicher anlassloser und jederzeit vorfallsbezogener Überprüfung)
2. **Schutz und Prävention**
3. **Erkennen** anormaler Aktivitäten
4. **Reaktion und Wiederherstellung** (BCM und Krisenmanagementfunktion)
5. **Lessons learned und Weiterentwicklung**
6. **Kommunikation** (intern und mit der Aufsicht)

- Erweiterte Pflichten der Geschäftsleiter (hinsichtlich Genehmigung, Überwachung und Überprüfung, inkl. regelmäßige Schulungen)
- Noch mehr Verschriftlichung als bisher schon (Anweisungen, Richtlinien und Prozesse)
- Erweiterte Meldepflicht bei IKT-Sicherheitsvorfällen (alle dadurch verursachten Kosten und Verluste, Klassifizierung der Vorfälle, um einheitliche Meldungen zu gewährleisten, Mehrfachmeldungen – Erstmeldung, Zwischenmeldung und Abschlussmeldung)
- Einsatz von auf dem neuesten Stand zu haltende IKT-Systeme, -Protokolle und –Tools

Gap-Analyse des Ist-Zustands mit dem Soll-Zustand erforderlich!

Bsp. Artikel 5 DORA Governance und Organisation

(1) Finanzunternehmen verfügen über einen internen Governance- und Kontrollrahmen, der im Einklang mit Artikel 6 Absatz 4 ein wirksames und umsichtiges Management von IKT-Risiken gewährleistet, um ein hohes Niveau an digitaler operationaler Resilienz zu erreichen.

(2) Das Leitungsorgan des Finanzunternehmens definiert, genehmigt, überwacht und verantwortet die Umsetzung aller Vorkehrungen im Zusammenhang mit dem IKT-Risikomanagementrahmen nach Artikel 6 Absatz 1. Für die Zwecke von Unterabsatz 1 gilt Folgendes:

a) Das Leitungsorgan trägt die letztendliche Verantwortung für das Management der IKT-Risiken des Finanzunternehmens;

b) das Leitungsorgan führt Leitlinien ein, die darauf abzielen, hohe Standards in Bezug auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten aufrechtzuerhalten;

c) das Leitungsorgan legt klare Aufgaben und Verantwortlichkeiten für alle IKT-bezogenen Funktionen sowie angemessene Governance-Regelungen fest, um eine wirksame und rechtzeitige Kommunikation, Zusammenarbeit und Koordinierung zwischen diesen Funktionen zu gewährleisten;

d) das Leitungsorgan trägt die Gesamtverantwortung für die Festlegung und Genehmigung der Strategie für die digitale operationale Resilienz gemäß Artikel 6 Absatz 8, einschließlich der Festlegung der angemessenen Toleranzschwelle für das IKT-Risiko des Finanzunternehmens gemäß Artikel 6 Absatz 8 Buchstabe b;

e) das Leitungsorgan genehmigt, überwacht und überprüft regelmäßig die Umsetzung der in Artikel 11 Absatz 1 genannten IKT-Geschäftsfortführungsleitlinie und der in Artikel 11 Absatz 3 genannten IKT-Reaktions- und Wiederherstellungspläne, die als eigenständige spezielle Leitlinie, die integraler Bestandteil der allgemeinen Geschäftsfortführungsleitlinie des Finanzunternehmens und seines Reaktions- und Wiederherstellungsplans ist, verabschiedet werden können;

f) das Leitungsorgan genehmigt und überprüft regelmäßig die internen IKT-Revisionspläne des Finanzunternehmens, die IKT-Revision und die daran vorgenommenen wesentlichen Änderungen;

g) das Leitungsorgan weist angemessene Budgetmittel zu und überprüft diese regelmäßig, um den Anforderungen des Finanzunternehmens an die digitale operationale Resilienz in Bezug auf alle Arten von Ressourcen gerecht zu werden, einschließlich einschlägiger Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz nach Artikel 13 Absatz 6 sowie IKT-Kompetenzen für alle Mitarbeiter; 27.12.2022 DE Amtsblatt der Europäischen Union L 333/29

h) das Leitungsorgan genehmigt und überprüft regelmäßig die Leitlinie des Finanzunternehmens in Bezug auf Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die von IKT-Drittdienstleistern bereitgestellt werden;

i) das Leitungsorgan richtet auf Unternehmensebene Meldekanäle ein, die es ihm ermöglichen, ordnungsgemäß über Folgendes informiert zu werden:

   i) mit IKT-Drittdienstleistern geschlossene Vereinbarungen über die Nutzung von IKT-Dienstleistungen,

   ii) alle relevanten geplanten wesentlichen Änderungen in Bezug auf die IKT-Drittdienstleister,

   iii) die potenziellen Auswirkungen derartiger Änderungen auf die kritischen oder wichtigen Funktionen, die Gegenstand dieser Vereinbarungen sind, einschließlich einer Zusammenfassung der Risikoanalyse, um die Auswirkungen dieser Änderungen zu bewerten, und zumindest über schwerwiegende IKT-bezogene Vorfälle und deren Auswirkungen sowie über Gegen-, Wiederherstellungs- und Korrekturmaßnahmen.

(3) […] (4) Die Mitglieder des Leitungsorgans des Finanzunternehmens halten ausreichende Kenntnisse und Fähigkeiten aktiv auf dem neuesten Stand — unter anderem indem sie regelmäßig spezielle Schulungen absolvieren — entsprechend den zu managenden IKT-Risiken, um die IKT-Risiken und deren Auswirkungen auf die Geschäftstätigkeit des Finanzunternehmens verstehen und bewerten können.

Bsp. 2. BAIT IT-Governance

2.1 Die IT-Governance ist die Struktur zur Steuerung sowie Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme einschließlich der dazugehörigen IT-Prozesse auf Basis der IT-Strategie. Hierfür maßgeblich sind insbesondere die Regelungen zur IT-Aufbau- und IT-Ablauforganisation (vgl. AT 4.3.1 MaRisk), zum Informationsrisiko- sowie Informationssicherheitsmanagement (vgl. AT 4.3.2 MaRisk, AT 7.2 Tzn. 2 und 4 MaRisk), zur quantitativ und qualitativ angemessenen Personalausstattung der IT (vgl. AT 7.1 MaRisk) sowie zum Umfang und zur Qualität der technischorganisatorischen Ausstattung (vgl. AT 7.2 Tz. 1 MaRisk). Regelungen für die IT-Aufbau- und IT-Ablauforganisation sind bei Veränderungen der Aktivitäten und Prozesse zeitnah anzupassen (vgl. AT 5 Tzn. 1 und 2 MaRisk).

2.2 Die Geschäftsleitung ist dafür verantwortlich, dass auf Basis der IT-Strategie die Regelungen zur IT-Aufbau- und IT-Ablauforganisation festgelegt und bei Veränderungen der Aktivitäten und Prozesse zeitnah angepasst werden. Es ist sicherzustellen, dass diese Regelungen wirksam umgesetzt werden.

2.3 Das Institut hat insbesondere das Informationsrisikomanagement, das Informationssicherheitsmanagement, den IT-Betrieb und die Anwendungsentwicklung quantitativ und qualitativ angemessen mit Ressourcen auszustatten.

2.4 Interessenkonflikte und unvereinbare Tätigkeiten innerhalb der IT-Aufbau- und IT-Ablauforganisation sind zu vermeiden.

2.5 Zur Steuerung der für den Betrieb und die Weiterentwicklung der IT-Systeme zuständigen Bereiche durch die Geschäftsleitung sind angemessene quantitative oder qualitative Kriterien durch diese festzulegen. Die Einhaltung der Kriterien ist zu überwachen.

Testen der digitalen operativen Resilienz

1. **Umfangreiche Vorgaben für Stresstests:** Um die Vorbereitung auf die Handhabung IKT-bezogener Vorfälle zu bewerten, Schwächen, Mängel und Lücken in Bezug auf die digitale operationale Resilienz zu erkennen und Korrekturmaßnahmen umgehend umzusetzen, erstellen, pflegen und überprüfen Finanzunternehmen […] ein solides und umfassendes Programm für das Testen der digitalen operationalen Resilienz als integraler Bestandteil des IKT-Risikomanagementrahmens.

2. Das in Artikel 24 genannte Programm für die Tests der digitalen operationalen Resilienz beinhaltet […] die Durchführung angemessener Tests, wie etwa Schwachstellen-bewertung und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests.

3. [Größere] Finanzunternehmen […] führen **mindestens alle drei Jahre** anhand von **TLPT** erweiterte Tests durch.

4. Auf der Grundlage des Risikoprofils des Finanzunternehmens und unter Berücksichtigung der betrieblichen Gegebenheiten kann die zuständige Behörde das Finanzunternehmen erforderlichenfalls auffordern, die Häufigkeit dieser Tests zu verringern oder zu erhöhen.

- Mind. jährliche Tests!
- Tests können intern oder extern beauftragt werden, müssen aber unabhängig sein.
- DORA sieht eine verhältnismäßige Umsetzung der Anforderungen an die Betriebsstabilitätstests in Abhängigkeit von der Größe sowie dem Geschäfts- und Risikoprofil der Finanzunternehmen vor.
- Die Tests reichen von Standardtests der IKT-Werkzeuge und -Systeme für kleinere Häuser bis hin zu fortgeschrittenen Tests auf der Grundlage von TLPT (Threat-Led Penetration Testing[1]) für bedeutende Finanzunternehmen.

Vielen Dank!

Dr. Verena Ritter-Döring

Partnerin, Banking & Finance Regulatory

Frankfurt am Main

+ 49 69 97130-404

v.ritter-doering@taylorwessing.com

Thomas Kahl

Partner, Technology, Media & Communications

Frankfurt am Main

+49 69 97130-241

t.kahl@taylorwessing.com

Europe > Middle East > Asia

taylorwessing.com