# DORA – Deltabetrachtung

## Was für die etablierte Finanzindustrie wirklich neu aus DORA ist

Dr. Waldemar Grudzien
Katrin Miller
Theresa Sporn
Moritz Treutwein

Oktober 2022
Blogpost

## Key Facts

- Bisherige BaFin-Aufsichtsobjekte sind gut gerüstet für DORA, neue DORA-Aufsichtsobjekte stehen vor großen Aufgaben
- Neu für BaFin-Aufsichtsobjekte sind 24 Anforderungen aus dem Verordnungstext und für alle DORA-Aufsichtsobjekte 19 RTS[1] sowie 2 ITS[2]
- Viele RTS/ITS können vorgezogen werden, Zuwarten auf finale Versionen wird nicht empfohlen
- Anforderungen können im Zeitverlauf mit RTS/ITS gebündelt und vorzeitig aufgelöst werden
- DORA untermauert Pro-Cloud-Entscheidung regulatorisch, denn ein „Aufsichtsschatten" ist mit DORA endgültig Geschichte

## 1. Einleitung

DORA soll zukünftig nationale Regelungen im Bereich der Finanzmarktregulierung in einheitliches, harmonisiertes EU-Recht überführen. CORE hat dazu bereits in einem ersten Blog-Post zu DORA Wesen, Inhalt, Auswirkungen und Empfehlungen dargelegt. Der vorliegende Blogpost ist eine Ergänzung des ersten und stellt auf das Delta zur aktuellen Regulierung ab, d.h. das, was für die etablierte Finanzindustrie tatsächlich neu aus DORA heraus ist.

DORA weitet den Geltungsbereich auf ca. 20 Arten von Unternehmen und IKT-Drittanbieter[3]. Für diejenigen Unternehmen, für die die Regelinhalte wie IKT-Risikomanagement, Meldung von IKT-Vorfällen und Prüfung der digitalen Betriebsstabilität bisher kein Thema waren, ist aus DORA heraus alles neu. Für die bereits durch die BaFin beaufsichtigten Unternehmen wie beispielsweise Kreditinstitute, Finanzdienstleistungsinstitute, Zahlungsinstitute und E-Geld-Institute, Versicherungsunternehmen, Wertpapierinstitute und Kapitalverwaltungsgesellschaften enthält

[1] Regulatory Technical Standards
[2] Implementing Technical Standards
[3] Ca. 20 Arten, da in der derzeitigen Trilog-Version vom 23.06.2022 im Vergleich zur vorherigen Version vom 26.09.2020 „Abschlussprüfer und Prüfungsgesellschaften" (Buchstabe q) rausgenommen wurden: a) Kreditinstitute, b) Zahlungsinstitute, c) E-Geld-Institute, d) Wertpapierfirmen, e) Anbieter von Krypto-Dienstleistungen, Emittenten von Kryptowerten, Emittenten von an Vermögenswerte geknüpften Token und Emittenten, signifikanter an Vermögenswerten geknüpfter Token, f) Zentralverwahrer, g) zentrale Gegenparteien, h) Handelsplätze, i) Transaktionsregister, j) Verwalter alternativer Investmentfonds, k) Verwaltungsgesellschaften, l) Datenbereitstellungsdienste, m) Versicherungs- und Rückversicherungsunternehmen, n) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, o) Einrichtungen der betrieblichen Altersversorgung, p) Ratingagenturen, ~~q) Abschlussprüfer und Prüfungsgesellschaften,~~ r) Administratoren kritischer Benchmarks, s) Crowdfunding-Dienstleister, t) Verbriefungsregister, u) IKT-Drittanbieter

DORA viele Anteile, welche diese bereits aus anderen regulatorischen Standards (siehe Abbildung 1) erfüllen müssen.

**Finanzunternehmen und IKT-Drittanbieter: Rechtsgrundlagen für Sonderprüfungen der technisch-organisatorischen Ausstattung**

| | Finanzunternehmen | Rechtsgrundlage für Sonderprüfung | Rechtsgrundlage für techn.-organ. Ausstattung | BaFin XAIT | BaFin Mindest-anforderungen (MaX) |
|---|---|---|---|---|---|
| I | Kreditinstitute, Finanzdienstleistungsinstitute | §44 Abs. 1 KWG | § 25a Abs. 1 KWG | BAIT vom 16.08.2021 | MaRisk vom 16.08.2021 |
| I | Zahlungsinstitute und E-Geld-Institute | § 19 Abs. 1 ZAG | § 27 Abs. 1 ZAG | ZAIT vom 16.08.2021 | Kein eigenes MaX-Dokument |
| II | Versicherungsunternehmen | § 306 Abs. 1 VAG | § 294 Abs. 4 VAG | VAIT vom 03.03.2022 | MaGo vom 02.03.2018 |
| III | Wertpapierinstitut | § 41 WpIG | - | BAIT vom 16.08.2021 | MaRisk vom 16.08.2021 |
| IV | Kapitalverwaltungsgesellschaften | § 14 KAGB (durch Verweis auf § 44 KWG) | §§ 28, 29 und 30 Kapitalanlagegesetzbuch (KAGB) | KAIT vom 01.10.2019 | KAMaRisk vom 10.01.2017 |
| V | IKT-Drittanbieter | Artikel 33, 34, 35 DORA (Entwurf vom 23.06.2022) | Artikel 1 DORA (Entwurf vom 23.06.2022) | - | - |

Quelle: CORE

Abbildung 1: Sonderprüfung in Finanzunternehmen – Rechtsgrundlagen und neues Aufsichtsobjekt IKT-Drittanbieter

Weitere für den genannten Kreis bekannte Regulierungsstandards sind das IT-Sicherheitsgesetz 2.0 mit den zwei zentralen Anforderungen „Mindestsicherheit der technisch-organisatorischen Ausstattung“ und „Meldewesen für schwerwiegende Sicherheitsvorfälle“ (nur für als KRITIS geltende Systeme), das Finanzmarktintegritätsstärkungsgesetz (FISG) mit Bestimmungen zur Anzeigepflicht für wesentliche Auslagerungen, die PSD 2 für Zahlungsdienstleister mit den RTS für erhöhte Sicherheitsanforderungen im Online-Zahlungsverkehr und das Geschäftsgeheimnisgesetz (GeschGehG) im Falle von Schadensersatzforderungen aus erfolgreichen Angriffen. Die gänzlich neuen Anteile werden im Nachgang besprochen.

Die neuen Anforderungen speisen sich aus den zwei Quellen Verordnungstext sowie den RTS und ITS. Auch die RTS und ITS sind Bestandteile der Verordnung, jedoch bilden sie durch ihre spätere Fertigstellung eine Klasse für sich. Mit dem Inkrafttreten der DORA wird zum Jahreswechsel 2022/23 gerechnet, die RTS/ITS folgen 12 bis 18 Monate später. Die Anwendung der DORA folgt zwei Jahre nach ihrem Inkrafttreten, sodass die Aufsichtsobjekte 6 bis 12 Monate Zeit für die Umsetzung der veröffentlichten RTS/ITS haben werden.

## 2. Handlungsbedarfe aus Text der Verordnung

In Abbildung 2 sind alle Anforderungen aus DORA zusammengestellt, die neu sind für die bisher schon durch die BaFin beaufsichtigten Aufsichtsobjekte aus XAIT[4] und MaX[5] – kurz: „DORA-Delta“. Im Anhang findet sich eine detaillierte tabellarische Aufstellung des DORA-Deltas.

**A bis B**: Übergreifend Anforderungen | **C bis M**: Anforderungen an IKT-Risikomanagement | **N bis O**: Meldung von IKT-Vorfällen | **P bis S**: Prüfung digitaler Betriebsstabilität | **T bis X**: Prüfung auf Risiko durch IKT-Drittanbieter

| Delta | Thema | Quelle |
|---|---|---|
| A | 8(2): CIA-Schutz von Daten und Systemen | Autoren-empfehlung |
| B | Aufbau zertifizierbares ISMS | Autoren-empfehlung |
| C | Erstellung separate „Strategie für digitale Resilienz“ | Artikel 5 (9) |
| D | Prüfung Option der Überprüfung der Einhaltung der Anforderungen an das IKT-Risikomanagement an Dritte zu delegieren | Artikel 5 (10) |
| E | Regelmäßige, jedoch mindestens jährliche, Bewertung des IKT-Risikos durch IKT-Altsysteme | Artikel 7 (7) |
| F | Erstellung „Policy für Informationssicherheit“ | Artikel 8 (4) |
| G | Erkennung von anomalen Aktivitäten, einschließlich IKT-Netzleistungsproblemen und IKT-Vorfällen & Erkennung von Anomalien von Handelsauskünften | Artikel 9 (1), Artikel 9 (4) |
| H | Erstellung „IKT-Strategie zur Fortführung des Geschäftsbetriebes“ | Artikel 10 (1) |
| I | Festlegung Krisenmanagementfunktion | Artikel 10 (6) |
| J | Meldung von Kosten und Verlusten aus IKT-Vorfällen an die zuständige Behörde (BaFin) | Artikel 10 (9) |
| K | Besondere Pflichten für Zentrale Gegenparteien und Zentralverwahrer bei Wiederherstellungs-plänen und dem sekundären Bearbeitungsstandort | Artikel 11 (3,4,5) |
| L | Meldung von Änderungen aus IKT-Vorfällen an die zuständigen Behörden | Artikel 12 (2) |
| M | Beauftragung von mindestens einer Person als Um-setzer der Kommunikationsstrategie und als Sprecher nach extern | Artikel 13 (3) |
| N | Alle Finanzunternehmen müssen schwerwiegende IKT-Vorfälle melden | Artikel 17 (1,3) |
| O | Hat oder könnte ein schwerwiegender IKT-Vorfall Auswirkungen auf Dienstnutzer und Kunden haben, müssen FU[1] diese unverzüglich unterrichten | Artikel 17 (2) |
| P | Etablierung eines Programms zur jährlichen Prüfung der digitalen Betriebsstabilität aller kritischen IKT-Systeme und -Anwendungen | Artikel 21 (6) |
| Q | Bedrohungsorientierte Penetrationstests | Artikel 23 |
| R | Prüfung Geeignetheit der Tester | Artikel 24 (1) |
| S | Einsatz interner Tester unterliegt drei Bedingungen | Artikel 24 (1a) |
| T | Erstellung „Strategie für Risiken durch IKT-Drittanbieter“ | Artikel 25 (3) |
| U | Unterrichtung der zuständigen Behörde über die geplante Vergabe von Aufträgen für kritische oder wichtige Funktionen | Artikel 25 (4) |
| V | Erstellung von Ausstiegsplänen und deren „ausreichende“ Erprobung | Artikel 25 (9) |
| W | Bewertung IKT-Konzentrationsrisiko | Artikel 26 |
| X | Wesentliche Vertragsinhalte | Artikel 27 |

Abbildung 2: Delta aus DORA-Entwurf vom 23.06.2022

[4] XAIT fasst BAIT, KAIT, VAIT und ZAIT zu einem Oberbegriff zusammen

[5] MaX fasst Mindestanforderungen an das Risikomanagement zusammen: MaRisk, MaGo und KaMaRisk

## 3. Handlungsbedarfe aus RTS / ITS

Abbildung 3 fasst alle aus DORA resultierenden RTS und ITS zusammen. Alle RTS und ITS werden 12 bis 18 Monate nach Inkrafttreten von DORA durch die ESA fertiggestellt, sodass die Aufsichtsobjekte theoretisch erst mit Verfügbarkeit dieser finalen Versionen mit der Umsetzung beginnen können. Aber das Vorziehen verschiedener RTS und ITS ist möglich und notwendig, um insgesamt besser auf die DORA vorbereitet zu sein als es der Wirtschaft zum Beispiel bei der DSGVO gelungen ist. Des Weiteren führt eine zeitliche Streckung aller RTS und ITS über die verfügbaren zwei Jahre zu einer komfortableren Bearbeitungssituation, als wenn mit den Arbeiten erst begonnen wird, wenn diese 21 Vorgaben bereitstehen. In diesem Fall hätten die Unternehmen für 8 RTS/ITS nur 6 Monate Zeit für die Umsetzung.

RTS ITS

| | Artikel | Thema RTS / ITS | Frist Bezug Inkrafttreten |
|---|---|---|---|
| 1 | 14(a) | 8(2): CIA-Schutz von Daten und Systemen | 1 Jahr nach |
| 2 | 14(d) | 8(4) lit. c: Rollen- und Rechtemanagement inkl. Zutritts- und Zugangsschutz, Überwachung anormalen Verhaltens | 1 Jahr nach |
| 3 | 14(e) | 9(1) (2): Erkennung IKT-bezogener Vorfälle, SIEM, SOC | 1 Jahr nach |
| 4 | 14(f) | 10(1): IKT-Plan für Fortführung desGeschäfts-betriebs als Bestandteil der operativen Strategie zur Fortführung des Geschäftsbetriebs | 1 Jahr nach |
| 5 | 14(g) | 10(5): Jährliche Überprüfung des IKT-Plans für die Wiederherstellung im Notfall sowie für die Fortführung des Geschäftsbetriebs | 1 Jahr nach |
| 6 | 14(h) | 10(3): Komponenten des IKT-Plans für Wiederherstellung im Notfall, der einer unabhängigen Prüfung zu unterziehen ist | 1 Jahr nach |
| 7 | 14(ha) | 5(6) Inhalt und Form des Berichts über die Überprüfung des IKT-Risikomanagementrahmens | 1 Jahr nach |
| 8 | 14a(3) lit. a bis e | Alle Inhalte aus 14a(1 lit. a,c,f,g), Inhalt und das Format des Berichts über die Überprüfung des IKT-Risikomanagementrahmens gemäß 14a(2) | 1 Jahr nach |
| 9 | 16(3) | 16(2) lit. a: Kriterien für Bestimmung schwerwiegender IKT-Vorfälle mit Meldepflicht, Proportionalitätsprinzip gemäß Artikel 31(2) | 1 Jahr nach |
| 10 | 16(3) | 16(2) lit. b: Kriterien zur Bedeutung der Relevanz schwerwiegender IKT-Vorfälle in anderen Ländern | 1 Jahr nach |
| 11 | 16(3) | 16(2) lit. c: U.a. Nutzer- und Transaktionszahlen berücksichtigen für Wesentlichkeitsschwellen erheblicher Cyber-Bedrohungen | 1 Jahr nach |

| | Artikel | Thema RTS / ITS | Frist Bezug Inkrafttreten |
|---|---|---|---|
| 12 | 18(1) lit. a | Inhalt von Berichten über schwerwiegende IKT-Vorfälle, Fristen und Inhalt für Meldungen | 18 Monate nach |
| 13 | 18(1) lit. b | Standartformulare, Vorlagen und Verfahren zur Meldung eines schwerwiegenden IKT-Vorfalles | 18 Monate nach |
| 14 | 23(4) | Details zu Penetrationstests gemäß TIBER-EU | 18 Monate nach |
| 15 | 25(10) | Standardvorlage für Informationsregister zu Verträgen mit IKT-Drittanbietern | 1 Jahr nach |
| 16 | 25(11) | Richtlinie zur Nutzung von IKT-Diensten inkl. Multi-Vendor-Strategie | 1 Jahr nach |
| 17 | 27(4) | (2) lit. a Beschreibung aller Funktionen und Dienstleistungen, die der IKT-Drittanbieter zu erbringen hat inkl. Zulässigkeit für Untervergaben | 18 Monate nach |
| 18 | 36(1) lit. a | Informationen für freiwilligen Antrag des IKT-Drittanbieters | 18 Monate nach |
| 19 | 36(1) lit. b | aus 31(1): Inhalt und Format für Abschlussberichte zur Umsetzung von Maßnahmen | 18 Monate nach |
| 20 | 36(1) lit. ca | aus 31(1): Informationen, inkl. Struktur, Formaten und Methoden, die ein IKT-Drittanbieter vorlegen muss; Kriterien für Zusammensetzung des Prüfungsteams inkl. Benennung, Aufgaben und Arbeitsmodalitäten | 18 Monate nach |
| 21 | 36(1) lit. d | aus 37(2): Bewertung der Maßnahmen der IKT-Drittanbieter zu Empfehlungen der federführenden Aufsichtsinstanz | 18 Monate nach |

Abbildung 3: aus DORA resultierende Regulatory Technical Standards (RTS) und Implementing Technical Standards (ITS)

Diejenigen technischen Standards, die Aufsichtsobjekte ohnehin bereits heute im Feld haben müssen, sollten zumindest aktualisiert werden, oder wenn nicht angemessen vorhanden, auf einen gesetzeskonformen Stand gebracht werden. Dazu gehören alle sieben RTS aus Artikel 14, denn mit dem Schutz der Vertraulichkeit, Integrität und Verfügbarkeit (CIA) müssen sich die bisherigen Aufsichtsobjekte der BaFin aus XAIT und MaX ohnehin befassen und alle neuen Aufsichtsobjekte aus DORA müss(t)en das aus Eigeninteresse ebenfalls schon tun. Für alle neuen Bestandteile aus einem RTS heraus, wie zum Beispiel Inhalt und Form des Berichts über die Überprüfung des IKT-Risikomanagementrahmens bietet sich Lobbyarbeit in der Form an, eigene Branchen-, Sektor-, Landesweite oder gar europäisch abgestimmte Entwürfe der ESA zur Verfügung zu stellen, sodass die „Überraschung“ bei der Vorlage der RTS durch die ESA möglichst klein bleibt.

Das gleiche gilt bei den drei RTS aus Artikel 16 rund um Meldungen zu schwerwiegenden IKT-Vorfällen und dem einen RTS und dem einen ITS aus Artikel 18 zu Berichten zu schwerwiegenden IKT-Vorfällen: erstens müssen sich alle zu Vorfällen verhalten und zweitens sollten der ESA die auszuarbeitenden Kriterien zuvor als abgestimmter Diskussionsvorschlag übermittelt werden. In diesem doppelten Sinne – eigene Umsetzung und Lobbyarbeit für einen möglichst europaweit,

aber zumindest national harmonisierten Diskussionsvorschlag an die ESA – können auch alle anderen RTS und ITS aus Abbildung 3 gesehen werden.

Auf das RTS aus Artikel 23 Absatz 4 zu Penetrationstests können Aufsichtsobjekte sich bereits jetzt vorbereiten, da die Verordnung das Testregime TIBER-EU favorisiert und dieses ist bekannt und verstanden. Einzig die Anforderungen an interne Tester könnten Überraschungen aus dem RTS mit sich bringen, sodass außer der Sicherung externer Testkapazitäten bereits heute die internen Testressourcen bis zum RTS weiterhin ihr Tagwerk verrichten.

Ebenso bekannt sind Register mit Verträgen zu Outsourcingunternehmen, sodass hier zum RTS aus Artikel 25 Absatz 10 nur eine Anpassung an das vorgegebene Format erfolgen muss. Die aus Artikel 25 Absatz 11 geforderte Richtlinie zur Nutzung von IKT-Diensten sollte schon heute Bestandteil eine ISMS sein und darf bisherige Aufsichtsobjekte vor keine größere Hürde stellen. Das sollte ebenfalls für die detaillierte Beschreibung aller Funktionen (Artikel 27 Absatz 4) des Outsourcingunternehmens gelten, andernfalls liefe bereits heute einiges falsch in den Verträgen zwischen BaFin-Aufsichtsobjekt und Hyperscaler. Mit dem freiwilligen Antrag des IKT-Drittanbieters zur Aufnahme in die Liste der zu überwachenden IKT-Drittanbieter (Artikel 36 Absatz 1 Buchstabe a) kann sich der Drittanbieter erst nach Erscheinen des entsprechenden RTS bemühen. Das gilt auch für die letzten drei Themenstellungen 19 bis 21 aus Abbildung 3: Adaptation an Gesetzestext ist erst mit Erscheinen der RTS sinnvoll.

## 4. Handlungsempfehlungen für bisherige Aufsichtsobjekte

In Abbildung 4 sind die RTS/ITS „1“ bis „21“ aus Abbildung 3 den Anforderungen aus dem Verordnungstext der DORA „A“ bis „X“ aus Abbildung 2 thematisch zugeordnet und gemeinsam über die Zeitachse aufgetragen. Die Annahme der Zeitplanung ist ein Inkrafttreten der DORA am 1. Januar 2023.

Den 21 RTS/ITS sind in Abbildung 4 noch zwei weitere „Fristsachen“ 22 und 23 aus dem Verordnungstext beigefügt. Diese sind zwar keine RTS/ITS, jedoch tragen sie zur weiteren Konkretisierung dieser bei:

- 22: Artikel 10 Abs. 9a: Gemeinsame Leitlinien der ESAs für die Schätzung der in Absatz 9 genannten aggregierten jährlichen Kosten und Verluste.
- 23: Bericht aus Artikel 19 Abs. 1 i.V.m. Abs. 3: Bericht zur Prüfung einer EU-Plattform für schwerwiegende IKT-Vorfälle

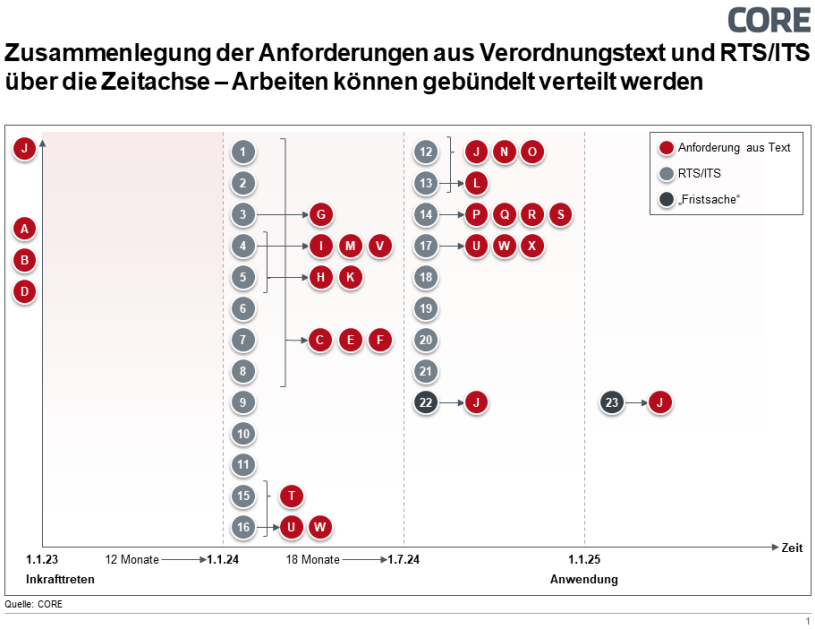


Abbildung 4: Zusammenlegung Verordnungsartikel und RTS/ITS über Zeitachse

Aus Abbildung 4 wird die Möglichkeit der Zusammenlegung der Anforderungen aus Verordnungstext und RTS/ITS über die Zeitachse kristallin, sodass die Arbeiten zur Konformität mit der DORA gebündelt und somit besser zeitlich wie organisatorisch verteilt werden können. Eine Betrachtung auf Gruppenebene eröffnet Räume der Fokussierung.

Gruppe A, B, D:

- A: Rechtzeitige Befassung mit Philosophie, Systematik und der Antizipation der DORA für eigene Organisation ist erfolgskritisch
- B: ein vollumfängliches ISMS müssen bisherige BaFin-Aufsichtsobjekte ohnehin in Betrieb haben – Check auf Aktualität empfohlen
- D: Prüfung der Option 2nd Line auszulagern kann im Vorfeld erfolgen

Gruppe C, E, F:

- C: Die Strategie für digitale Resilienz umfasst alle Anforderungen des Artikel 14 DORA und damit 8 RTS – im Rahmen der Aktualisierung des ISMS zu erledigen
- E: Basierend auf eigener Definition Identifikation der IKT-Altsysteme und gemeinsame Abhandlung in Strategie aus C)
- F: Policy für Informationssicherheit ist aus vorhandener IT-Strategie und neuer Strategie aus C) abzuleiten

Gruppe I, M, V:

- I: Festlegung der Krisenmanagementfunktion in der operativen Strategie zur Fortführung des Geschäftsbetriebs
- M: Festlegung Funktion Implementierer der Kommunikationsstrategie in der operativen Strategie zur Fortführung des Geschäftsbetriebs

- V: Ausstiegspläne und deren Erprobung eingebettet in der operativen Strategie zur Fortführung des Geschäftsbetriebs

Gruppe H, K:

- H: Erstellung IKT-Strategie zur Fortführung des Geschäftsbetriebes und deren Überprüfung entlang der Leitplanken aus RTS 4 und RTS 5
- K: Besondere Pflichten für sekundären Bearbeitungsstandort für Zentralverwahrer und Zentrale Gegenparteien entlang der Leitplanken aus RTS 4 und RTS 5

Gruppe U, W und X:

- U: Meldung von Outsourcing/-Vorhaben zwar aus FISG bekannt, jedoch werden RTS 16 und RTS 17 neue Anforderungen stellen
- W: Bewertung des IKT-Konzentrationsrisikos insb. Ohne RTS 16 schwer früher zu erstellen
- X: RTS 17 wird neue Vorgaben für wesentliche Vertragsinhalte aufstellen

Gruppe J, N, O:

- J: sofortige Lobbyarbeit gegen Fristsache 23 empfohlen; mit RTS 12 und RTS 13 sowie Fristsache 22 werden Inhalt und Format dieser Meldung vorgegeben
- N: sofortige Lobbyarbeit notwendig; mit RTS 12 und RTS 13 werden Inhalt und Format dieser Meldung vorgegeben
- O: sofortige Lobbyarbeit notwendig; mit RTS 12 und RTS 13 werden Inhalt und Format dieser Meldung vorgegeben

Gruppe P, Q, R, S:

- P: Ausarbeitung des Prüfprogramms muss sofort aufgenommen werden, RTS 14 wird Penetrationstests ausdetaillieren
- Q: Ausarbeitung Vorgehen zur ausreichenden Ausstattung mit externen und wenn vorgesehen auch internen Testkapazitäten; Ausarbeitung der Testung an Live-Systemen, frühzeitige Sicherung von Testkapazitäten empfohlen
- R: Auswahl und Sicherung der Tester unter Einbezug von RTS 14 – aber Orientierung an TIBER EU bereits jetzt möglich und empfohlen
- S: Entscheidung ob interne Tester noch sinnvoll im Lichte der Anforderungen

Einzel-Deltas:

- G: Anomalienerkennung mit RTS 3 verbinden
- L: Meldung von Lessons Learned bedarf keine vorzeitigen Aktionen
- T: Strategie für Risiken durch IKT-Drittanbieter mit Vorgaben zur Multi-Vendor-Strategie aus RTS 16 zu verbinden; RTS 15 wird das Vertragsregister strukturieren

## Fazit

DORA wird den Aufsichtsrahmen auf ca. 20 Unternehmensarten weiten und damit endlich den Fokus Europas auf die wichtigste Ressource für Wohlstand und Gestaltungsfreiheit in einer überkomplexen Welt richten – die digitale Infrastruktur. Finanzunternehmen und IKT-Drittanbieter bilden dabei den Startpunkt für eine moderne, automatisierte Aufsichtspraxis. Weitere wichtige Sektoren werden folgen.

Beide, die bisherigen BaFin-Aufsichtsobjekte als auch die alle neuen DORA-Aufsichtsobjekte können es sich Summa summarum nicht erlauben auf die Fertigstellung der RTS und ITS durch die ESA gegen Ende 2023 und gegen Mitte 2024 zu warten. Wie oben erläutert, bleibt in diesem Falle den Unternehmen maximal ein Jahr Zeit, für 8 RTS/ITS sogar nur 6 Monate, für die Umsetzung. Zweitens blockieren diese notwendigen aufsichtlichen Arbeiten die Linientätigkeiten für viele Monate ungebührend; eine zeitliche Streckung von 6 Monaten auf bis zu zwei Jahre ist erfolgsversprechender als ein Zuwarten. Vielmehr müssen beide Gruppen bereits jetzt mit den Vorbereitungen auf diese beginnen. Dann haben sie erstens die Chance gesetzeskonform zu bleiben und zweitens können sie auf Basis ihrer Lessons learned aus DORA den ESAs rechtzeitig Diskussionsangebote für einzelne RTS und ITS unterbreiten, um noch Einfluss auf die Ausgestaltung von Details in Governance und Organisation ihrer digitalen Produktionsbasis nehmen zu können.

Abseits der regulatorischen Politiken und des aufsichtlichen „Kleins-Kleins“ stellen sich neue Erkenntnisse und Fragen mit der DORA ein. Zunächst einmal der Gemeinplatz: Banken-Aufsicht ist IT-Aufsicht! Diese Erkenntnis sollte nun überall angekommen sein. Spätestens mit DORA verschwindet der „Aufsichtsschatten“, den die Aufsichtsobjekte in den ersten Jahren des Outsourcings in die Cloud hatten. Im Umkehrschluss bedeutet das aber, dass ein Outsourcing in die Cloud wohl durchdacht und kalkuliert ist, denn der Gang in die Cloud wird nur sinnvoll bei wirklichem Mehrwert, da der „Vorteil“ geringerer Compliance-Anforderungen in der Cloud mit DORA nicht mehr gegeben ist. Wenn ein Unternehmen nun nach den Bedingungen der DORA outsourct, dann ist die Erfolgswahrscheinlichkeit des Outsourcings wegen DORA größer als ohne DORA. Ein Umkehrschluss in Richtung Aufsicht: Wenn die gleiche Aufsicht Finanzunternehmen und IKT-Drittanbieter nach gleichen Regeln beaufsichtigt, warum müssen Finanzunternehmen diese IKT-Drittanbieter so steuern und überwachen, als ob diese nicht beaufsichtigt wären?

## 5. Anhang: Neuerungen aus DORA für BaFin-Aufsichtsobjekte

| Lit. | Neues Handlungsfeld | Beschreibung / Folgerung | Quelle |
|---|---|---|---|
| **Übergreifende Anforderungen** | | | |
| A | Erstellung Zeit- und Maßnahmenplan für alle noch zu erstellenden RTS | Eine frühzeitige Vorbereitung auf die Themenstellungen der RTS und ITS (siehe Kapitel 0) bereits VOR deren Fertigstellung wird dringend empfohlen. | Empfehlung der Autoren |
| B | Aufbau zertifizierbares ISMS | ISMS in DORA-Version vom 23.06.2022 nicht mehr gefordert, allerdings fordert DORA in Praxis ein voll umfänglich aufgebautes ISMS).<br>Bisher fordern die XAIT-Anforderungen jeweils in der Vorbemerkung den Betrieb eines ISMS, aber nicht eines zertifizierten ISMS. Damit das ISMS allen aufsichtlichen Anforderungen genügt, muss es zertifizierungsfähig sein, d.h. „als ob“ eine Zertifizierung zum Beispiel gemäß ISO 27001 das Ziel wäre. Zweitens gehen die Autoren davon aus, dass in einer weiteren Regulierungsrunde ein zertifiziertes ISMS für die kritischen Prozesse vorgeschrieben wird. | Empfehlung der Autoren |
| **Anforderungen an IKT-Risikomanagement (Artikel 5 bis 14)** | | | |
| C | Erstellung separate „Strategie für digitale Resilienz“ | Betonung digitale Resilienz. Diese neu geforderte Strategie ist Teil des IKT-Risikomanagementrahmens und vereint bereits bekannte Inhalte aus Dokumenten wie IT-Strategie, Informationssicherheitsleitlinie und Auslagerungsrichtlinie. Jedoch muss diese Strategie als eigenständiges Dokument verfasst sein, die Geschäftsstrategie in die IKT fortführen und speziell auf die IKT-Risiken fokussieren. | Artikel 5 (9) |
| D | Prüfung der Option die Überprüfung der Einhaltung der Anforderungen an das IKT-Risikomanagement an Dritte zu delegieren. | Finanzunternehmen können die genannte Überprüfung nach extern delegieren und so bspw. die Interne Revision entlasten. | Artikel 5 (10) |
| E | Regelmäßige Bewertung des IKT-Risikos durch IKT-Altsysteme | Das Finanzunternehmen muss klären welche Teile der Infrastruktur als IKT-Altsysteme gelten. Der Hinweis aus DORA „vor und nach Anschluss alter und neuer Technologien, Anwendungen oder Systeme“ verlagert die Abgrenzung „alt/neu“ auf weitere Komponenten einer Infrastruktur. | Artikel 7 (7) |
| F | Erstellung „Policy für Informationssicherheit“ | Diese Policy soll die Regeln zum Schutz der CIA-Schutzziele vorgeben und ist somit eher als Richtlinie denn als Strategie zu verstehen. In praxi verfügt jedes beaufsichtigte Finanzunternehmen über diese Regeln in Form des Sollmaßnahmenkatalogs (TMC) und der dazugehörigen Kontrollen sowie in Richtlinien und Arbeitsanweisungen zum Schutz der Vermögenswerte (‚Assets‘), jedoch wird dieses Dokument explizit genannt, sodass | Artikel 8 (4) |

| Lit. | Neues Handlungsfeld | Beschreibung / Folgerung | Quelle |
|---|---|---|---|
| | | es als übergeordnete „Klammerpolicy“ erstellt werden muss, als separate Strategie oder ggf. als Teil der IT-Strategie. | |
| G | Erkennung von anomalen Aktivitäten, einschließlich IKT-Netzleistungsproblemen und IKT-Vorfällen | Neu wenn Aufsicht darunter immer ein SIEM und/oder SOC versteht | Artikel 9 (1) |
| | Erkennung von Anomalien von Handelsauskünften | Neu, nur für Wertpapierfirmen. Diese müssen sich gemäß MiFIR so genannter Genehmigter Veröffentlichungssysteme (Approved Publication Arrangement – APA) bedienen und können so genannte Genehmigte Meldemechanismen (Approved Reporting Mechanism – ARM) nutzen. | Artikel 9 (4) |
| H | Erstellung „IKT-Strategie zur Fortführung des Geschäftsbetriebes“ | Auch die Bestandteile dieser „Strategie“ müssen bereits heute im BCMS (Business Continuity Management) vorhanden sein, jedoch erachtet die Aufsicht die IKT-Bestandteile als so betriebskritisch, dass sie nun herausgestellt werden. Aus Sicht der Autoren kann diese IKT-Strategie Bestandteil der BCM-Strategie sein und ausschließlich IT-Inhalte adressieren. | Artikel 10 (1) |
| I | Festlegung Krisenmanagementfunktion | Diese Funktion ist die typische BCM-Managementfunktion, ist jetzt aber gesetzlich vorgeschrieben. | Artikel 10 (6) |
| J | Meldung von Kosten und Verlusten aus IKT-Vorfällen an die zuständige Behörde | Seit Jahrzehnten politisch verhindert (Stichwort UP KRITIS). Finanzunternehmen müssen intern klären nach welcher Metrik sie IKT-Vorfälle, Kosten und Verluste zusammenstellen können. Extern bleibt die Frage nach den Gefahren aus dieser zentralen Sammlung. Hier wird Lobbyarbeit über Verbände und weitere Industriezusammenschlüsse als politische Flankierung notwendig sein. | Artikel 10 (9) |
| K | Besondere Pflichten für Zentrale Gegenparteien und Zentralverwahrer bei den Wiederherstellungsplänen und dem sekundären Bearbeitungsstandort | Detailvorgaben für Backups, Wiederanlauf und zweitem Bearbeitungsstandort für zwei der 20 Arten von Finanzunternehmen. | Artikel 11 (3,4,5) |
| L | Meldung von Änderungen aus IKT-Vorfällen an die zuständigen Behörden | Diese Meldung von Lessons Learned aus IKT-Vorfällen an die zuständigen Behörden ist neu und versetzt diese besser in die Lage „am Puls der Zeit“ bei Angriffs- und Bedrohungsgeschehen ihrer Aufsichtsobjekte zu sein. | Artikel 12 (2) |
| M | Beauftragung von mindestens einer Person als Umsetzer der Kommunikationsstrategie und als Sprecher nach extern. | Die Kodifizierung einer verantwortlichen Rolle als „öffentlicher Sprecher und Medienspecher“ ist neu. Große Unternehmen verfügen auch heute über Pressesprecher. Viele aus DORA neu beaufsichtigte Unternehmen werden diese Rolle überhaupt erst benennen müssen. | Artikel 13 (3) |

| Lit. | Neues Handlungsfeld | Beschreibung / Folgerung | Quelle |
|---|---|---|---|
| N | Alle Finanzunternehmen müssen schwerwiegende IKT-Vorfälle melden. | Bisher müssen nur KRITIS-Betreiber gemäß IT-Sicherheitsgesetz i.V.m. BAIT Kapitel 12 resp. VAIT Kapitel 11 resp. ZAIT Kapitel 12 schwerwiegende IKT-Vorfälle an die zuständige Behörde melden. Mit DORA wird dieser meldepflichtige Kreis auf alle Finanz-unternehmen gemäß Artikel 2 Abs. 2 erweitert. | Artikel 17 (1, 3) |
| O | Unterrichtung über IKT-Vorfall: Wenn ein schwerwiegender IKT-Vorfall Auswirkungen auf Dienstnutzer und Kunden hat oder haben könnte, müssen FU diese unverzüglich unterrichten. | Dienstnutzer und Kunden müssen über schwerwiegenden IKT-Vorfall unterrichtet wer-den. Diese Informationspflicht ist bisher nur aus der DSGVO bekannt, nun wird sie mit DORA auch auf die Informations- und Cybersicherheit erweitert. | Artikel 17 (2) |
| P | Etablierung eines Programms zur jährlichen Prüfung der digitalen Betriebsstabilität aller kritischen IKT-Systeme und -Anwendungen. | Neu sind zwei sehr wichtige Aspekte: erstens – mit einer Ausnahme – der jährliche Turnus der Prüfung und zweitens muss die Prüfung alle kritischen Systeme und Anwendungen umfassen. Das findet sich bisher in der deutschen Regulierung nicht in dieser Rigorosität wieder: In BAIT Tz. 5.6 und ZAIT Tz. 5.6 ist die Rede von „den IT-Systemen“ (und nicht „allen IT-Systemen“) und der „regelmäßigen“ Überprüfung. Die Ausnahme findet sich in der VAIT Tz. 5.6, nach der Versicherungsunternehmen bereits heute „kritische Systeme …mindestens jährlich“ überprüfen müssen. | Artikel 21 (6) |
| Q | Bedrohungsorientierte Penetrationstests | Bisher sind bedrohungsorientierte Penetrationstests aus TIBER-EU bekannt und in Deutschland ist die Teilnahme an TIBER-DE freiwillig.<br><br>Nun werden bedrohungsorientierte Penetrationstests zur Pflicht. Sie müssen für kritische und wichtige Funktionen mindestens alle drei Jahre durchgeführt werden, auch an ausgelagerten Funktionen. Die Tests werden an Live-Produktionssystemen durchgeführt. Die zuständige Behörde muss im Vorfeld den Umfang des Penetrationstests genehmigen und nach Durchführung auch die ordnungsgemäße Durchführung bescheinigen.<br><br>Bei Nutzung interner Tester müssen alle 3 Tests externe Tester eingebunden werden. | Artikel 23 |
| R | Prüfung Geeignetheit der Tester | Aus den umfangreichen Anforderungen an die Prüfer muss die Empfehlung der frühzeitigen Sicherung von Prüfungskapazitäten abgeleitet werden. Auch für die Prüfer sind die Anforderungen aus DORA neu, sodass mit Anwendung von DORA voraussichtlich in Q3 2025 das Angebot an DORA-konformen Prüfern den Bedarf nicht decken können wird. | Artikel 24 |

| Lit. | Neues Handlungsfeld | Beschreibung / Folgerung | Quelle |
|---|---|---|---|
| S | Einsatz interner Tester unterliegt Bedingungen | Große Hürden vor dem Einsatz von internen Testern durch drei Bedingungen:<br>- Sie müssen durch die zuständige Behörde genehmigt werden;<br>- zuständige Behörde prüft auf ausreichende Ressourcen und auf Vermeidung von Interessenskonflikten während der gesamten Planungs- und Durchführung des Tests;<br>- der „Threat Intelligence“-Anbieter ist nicht mit dem Finanzunternehmen verbunden | Artikel 24 (1a) |
| T | Erstellung „Strategie für Risiken durch IKT-Drittanbieter“, enthält u.a. Vertragsregister zu IKT-Drittanbietern | Diese Strategie kann im Prinzip als bisher schon den BaFin-Aufsichtsobjekten hinlänglich bekannte Auslagerungsstrategie gesehen werden – hier mit Fokus auf „IKT-Drittanbieter“. Für alle neuen Aufsichtsobjekte der DORA wird das hingegen eine neue und nicht einfach zu erfüllende Aufgabe. Inwieweit die BaFin diese neue Strategie als separate Strategie einfordert oder sie als Teil einer bestehenden Strategie akzeptiert, wird sich nach Inkrafttreten von DORA zeigen. | Artikel 25 (3) |
| U | Information der zuständigen Behörde über die geplante Vergabe von Aufträgen für kritische oder wichtige Funktionen | Auch diese Forderung ist den bisherigen BaFin-Aufsichtsobjekten seit Anfang des Jahres durch das FISG bekannt, sodass eine Adaptation an DORA keinen übermäßigen Aufwand darstellen sollte, wie es das für neue Aufsichtsobjekte der DORA sein wird.<br>Die nachträgliche Information bei Hochstufung einer Funktion als kritisch oder wichtig ist für bisherige BaFin-Aufsichtsobjekte ebenfalls aus dem FISG bekannt. | Artikel 25 (4) |
| V | Erstellung von Ausstiegsplänen | In der Entwurfsfassung von DORA vom 24.09.2020 sollten die Ausstiegspläne noch „gegebenenfalls ausreichend erprobt“ sein, was hinreichend unbestimmt war. In dem Trilog-Kompromisstext vom 23.06.2022 müssen die Ausstiegspläne umfassend, dokumentiert und im Sinne des Proportionalitätsprinzips nach Artikel 3a Abs. 2 ausreichend getestet und regelmäßig überprüft werden. Die neue Formulierung verringert die Unbestimmtheit. Gleichwohl ist die „ausreichende Testung“ von Ausstiegsplänen für alle Finanzunternehmen eine sehr große Herausforderung. Ein Beispiel: Wie soll eine Bank ihren Hyperscaler ausreichend testen? | Artikel 25 (9) |
| W | Bewertung IKT-Konzentrationsrisiko | Alle Finanzunternehmen müssen vor einer potenziellen Auslagerung das IKT-Konzentrationsrisiko bewerten. Diese gänzlich neue Anforderung stellt alle Finanzunternehmen vor eine hohe Hürde. Sie müssen verschiedene Aspekte berücksichtigen wie „leichte Ersetzbarkeit“, „mehrfach vertragliche Vereinbarungen mit demselben/eng verbundenen IKT-Drittanbieter“. Zudem müssen | Artikel 26 |

| Lit. | Neues Handlungsfeld | Beschreibung / Folgerung | Quelle |
|---|---|---|---|
| | | Alternativen untersucht und Risiken durch Unterauftragnehmer der IKT-Drittanbieter bewertet werden. Des Weiteren müssen Finanzunternehmen auch bewerten, ob die Aufsichtsbehörde mit der Auslagerungskette in der Lage ist, das Finanzunternehmen zu beaufsichtigen.<br><br>Der Artikel besteht aus Unwägbarkeiten, erst die (Prüfungs-)Praxis wird zeigen, ob und wie diese Anforderungen umgesetzt werden können. | |
| X | Wesentliche Vertragsbestimmungen | Beachtung von Mindestinhalten des Vertrages zwischen Finanzunternehmen und IKT-Drittanbietern, u.a. müssen Kündigungsrechte „den Erwartungen der zuständigen Behörde entsprechen“. Diese „Erwartungen der Aufsicht“ sind heute nicht abschätzbar. Sind diese von Land zu Land unterschiedlich oder europäisch einheitlich? | Artikel 27 |

## Verfasser

**Waldemar Grudzien** ist Expert Partner bei CORE und Gründer der Regulation and Compliance Practice. Er wurde in Elektrotechnik promoviert und verfügt über ein Diplom in VWL. Schwerpunkte seiner Arbeit sind Informationssicherheit und Datenschutz – in Theorie und Praxis, inklusive der Tätigkeit als ISB und DSB in verschiedenen Klientensituationen. Er unterstützt Klienten im Aufbau und sicherem Betrieb zertifizierungsfähiger ISMS.

**Mail:** waldemar.grudzien@core.se

**Katrin Miller** ist **Legal Expertin** bei CORE. Sie bringt umfangreiche Erfahrungen aus Informationssicherheitsprojekten im Finanzsektor mit; insbesondere über Anwendungskenntnisse zu den Themenstellungen Informationsrisikomanagement, BIA (Business Impact Analysis) und SBF (Schutzbedarfsfeststellung). Frau Miller beschäftigt sich auch mit Geldwäscheprävention.

**Mail:** katrin.miller@core.se

**Theresa Sporn** ist Expert Fellow bei CORE und verfügt über einen Bsc. in Management. Sie hat während ihres Studiums Arbeitserfahrung im Consulting- und anschließend im Data Science Bereich eines HR Tech Unternehmens gesammelt und unterstützt das Team bei CORE mit Datenanalysen und Visualisierung.

**Mail:** theresa.sporn@core.se

**Moritz Treutwein** ist **Transformation Manager** bei CORE. Sein Beratungsschwerpunkt ist Banking & Capital Markets, dabei umfasst seine Expertise unter anderem die Steuerung und Umsetzung von Geschäftsfelderweiterungen im Rahmen von IT-Implementierungsprojekten, Audit Remediations, sowie die Entwicklung digitaler Geschäftsmodelle. Darüber hinaus ist er Informationssicherheitsbeauftragter bei CORE.

**Mail:** moritz.treutwein@core.se

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633
office@core.se