DORA – Regulation der Technologien im Finanzsektor

Neuordnung der IKT-Regulierung von Finanzunternehmen und ihren Dienstleistern

Dr. Waldemar Grudzien
Nadine Hofmann
Holger Friedrich

August 2022
Blogpost

Key Facts

- Mit dem **D**igital **O**perational **R**esilience **A**ct (DORA) will die EU den Finanzsektor widerstandsfähiger gegen IT-Störungen und Cyberangriffe machen
- DORA liegt im Entwurf vor, Trilog Verfahren noch nicht abgeschlossen, Inkrafttreten wohl nicht in diesem Jahr
- DORA wird bestehende Anforderungen an Risikomanagement moderner Technologien EU-weit harmonisieren
- IKT-Drittanbieter wie beispielsweise Hyperscaler oder Corebanking-Provider werden zukünftig in gleicher Art geprüft, wie bisherige Aufsichtsobjekte Banken und Versicherungen
- Hyperscaler werden zentral durch ESA und die nationale Aufsicht geprüft und zahlen für Aufsichtstätigkeit
- DORA wird mehr MINT-Expertise in den Leitungs- und damit auch Aufsichtsgremien erfordern
- Zertifizierungsfähige Informationssicherheitsmanagementsysteme (ISMS) werden europäische Best Practice im Finanzsektor
- Zukünftig erhöhte Verwaltungsaufwände durch neue Berichtspflichten und Genehmigungsverfahren
- Als kritisch deklarierte Finanzunternehmen werden turnusmäßig ihre digitale Betriebsstabilität durch bedrohungsorientierte Penetrationstests beweisen
- Hybride IT-Prüfung als Standard für manuell-automatisierbare Prüfungshandlungen zu etablieren

Einleitung

Mit dem „**D**igital **O**perational **R**esilience **A**ct" (DORA) wird ein EU-Rechtsrahmen „über die Betriebsstabilität digitaler Systeme des Finanzsektors" erschaffen. Grundsätzlich fasst DORA bestehende Regelungen zu Sicherheitsmaßnahmen, Meldewesen und Überprüfung von Auslagerungen zusammen, erweitert und vertieft diese jedoch an ausgewählten Stellen. IKT[1]-Drittanbietern werden inkludiert, womit der so genannten federführenden Aufsichtsinstanz (je nach Art des Aufsichtsobjekts EBA, ESMA oder EIOPA) durch Möglichkeiten der Intervention wie bspw. Zwangsgeldern die nötigen Mittel zu Durchsetzung von Standards in der Finanzmarktstabilität an die Hand gegeben werden. Als umfassendes Regelwerk für die Informationssicherheit wird DORA in den drei Dimensionen Organisation, Regulatorik und IT in Finanzunternehmen eine vergleichbar große Wirkung entfalten wie die DSGVO im Schutz persönlicher Daten seit ihrer Geltung im Mai 2018. Während die DSGVO für die gesamte Wirtschaft und Verwaltung gilt, aber nur den Schutz personenbezogener Daten adressiert, wird DORA „nur" für alle Finanzunternehmen gelten – hierunter fallen auch diverse Verwaltungsentitäten, allerdings hat DORA den Schutz aller Informationen zum Ziel, die personenbezogenen Daten eingeschlossen. Abbildung 1 spannt

[1] Informations- und Kommunikationstechnologie

illustrativ den Rahmen in den drei Dimensionen Organisation, Regulatorik und IT für die drei Entitäten 3. Säule, 4. Säule (Neobanken) und Regulator auf.

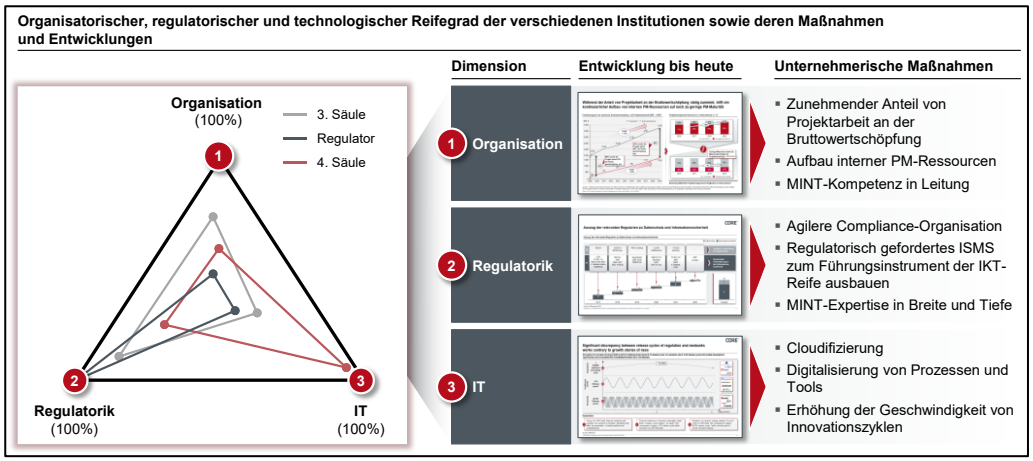


Abbildung 1: DORA greift in Reifegrad einer Organisation in den drei Dimensionen Organisation, Regulatorik und IT ein

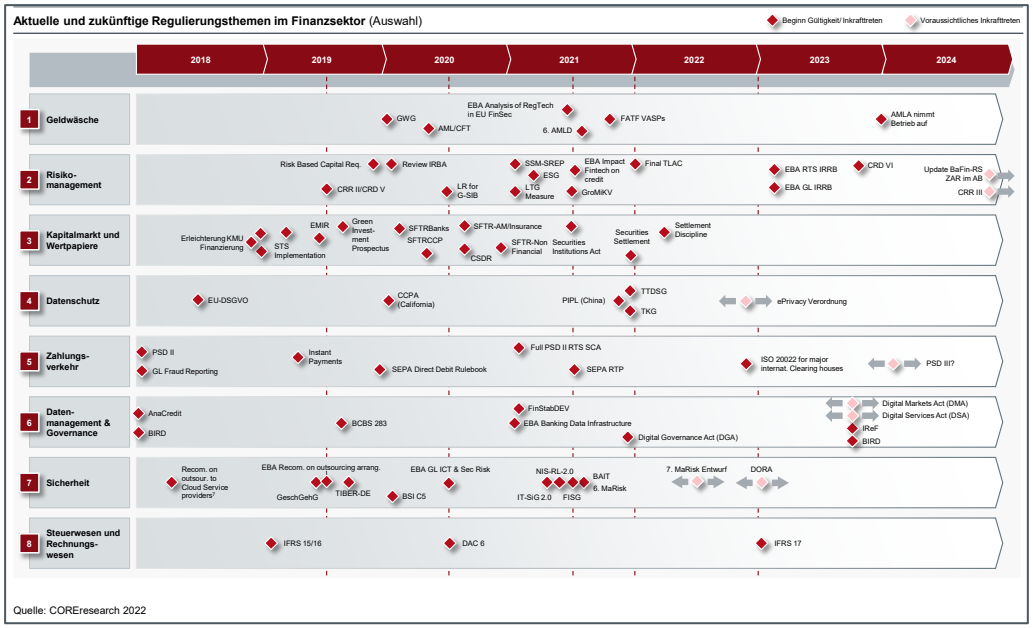
Es gelten zwar die europäischen Vorschriften mit Regelungen zur IKT-Sicherheit und Meldewesen im Finanzsektor wie NIS-Richtlinie, DSGVO, PSD 2 inklusive diverser RTS (Regulatory Technical Standards) und Implementing Technical Standards (ITS) in jedem Mitgliedsland des europäischen Wirtschaftsraums, jedoch legen eine Vielzahl von Ländern, so auch Deutschland, diese Vorgaben national aus. In Deutschland muss der Finanzsektor legale Anforderungen rund um die Informationssicherheit sowie das Risikomanagement aus MaRisk[2], XAIT[3] (BAIT[4] / KAIT[5] / VAIT[6] / ZAIT[7]), GeschGehG[8], FISG[9] und IT-SiG[10] 2.0 erfüllen (siehe Abbildung 2). Diese „Mehrfachregulierung“ der gleicher IKT in verschiedenen Regelwerken provoziert Ineffizienzen bis hin zu Ineffektivitäten aufgrund von Überschneidungen, Inkonsistenzen und mehrfachen Vorgaben zur Sicherheit der IKT.

Intendiert scheint, dass DORA europäische und nationale Vorschriften harmonisieren sowie potenziell obsolet machen soll. Es wird sich zeigen, ob die Mitgliedsstaaten auf eigene Regelungen verzichten, da Verwaltungsstrukturen einmal erreichte Machtgefüge selten widerstandslos aufgeben. Hier setzt DORA an und ermöglicht grenzüberschreitend tätigen Finanzunternehmen durch vergleichbare Vorschriften und die EU-weite Anerkennung von Prüfungen das internationale Geschäft erleichtern. Daher ist der DORA-Entwurf aus Perspektive einer weitergehenden europäischen Integration sowie der Steigerung der Wettbewerbsfähigkeit der Teilnehmer im europäischen Finanzplatz zu unterstützen.

Im Folgenden wird der Inhalt der DORA eingehend vorgestellt. Es werden Herausforderungen für den Finanzsektor aus Sicht der Autoren aufgezeigt. Folgend sind Hinweise zur Herstellung der Compliance zu DORA angerissen.

[2] Mindestanforderungen an das Risikomanagement – MaRisk, Version 16.08.2021
[3] XAIT subsumiert alle Rundschreiben der BaFin zu aufsichtlichen Anforderungen an die IT
[4] Bankaufsichtliche Anforderungen an die IT (BAIT), Version 16.08.2021
[5] Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT), Version 01.10.2019
[6] Versicherungsaufsichtliche Anforderungen an die IT (VAIT), Version 03.03.2022
[7] Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten (ZAIT), Version 16.08.2021
[8] Geschäftsgeheimnisgesetz
[9] Gesetz zur Stärkung der Finanzmarktintegrität
[10] IT-Sicherheitsgesetz (auch als BSI-Gesetz bekannt)

Die DORA subsummiert Anforderungen an die Sicherheit im Finanzsektor, weitet den Kreis der Aufsichtsobjekte aus und stellt in einzelnen Sicherheitsbereichen neue und höhere Anforderungen auf.



Quelle: COREresearch 2022

Abbildung 2: Regulierungsrahmen für den Finanzsektor, Sicherheit (Zeile 7) im Fokus, DORA im Zentrum

Inhalt der DORA

Während die drei Artikelblöcke „Anforderungen an IKT-Risikomanagement", „Meldung von IKT-Vorfällen" sowie „Prüfung der digitalen Betriebsstabilität" Finanzunternehmen und damit auch IKT-Drittanbieter adressieren, reguliert der Artikelblock „Prüfung des Risikos durch IKT-Drittanbieter" einzig die Technologieanbieter. Mit 15 Artikeln werden detailliert die Anforderungen an IKT-Drittanbieter wie beispielsweise Hyperscaler[11] formuliert. Auch Funktionsanbieter für Kernbankensystemlösungen[12] werden in den Geltungsbereich einbezogen.

Geltungsbereich (Artikel 2)

Die DORA weitet den Regulierungsrahmen von den „klassischen" Regulierungsobjekten Kreditinstitute, Zahlungsinstitute, E-Geld-Institute, Wertpapierfirmen auf insgesamt 21 verschiedene Arten von Finanzunternehmen[13] auf. Besonders bedeutsam ist dabei das neue Regulierungsobjekt „IKT-Drittanbieter".

Das Feld der Aufsichtsobjekte wird deutlich vergrößert und stellt die Aufsichtsstrukturen vor neue quantitative und qualitative Aufgaben. Zudem müssen Finanzunternehmen, die als bedeutend

[11] Bspw. Amazon Azure, Microsoft Azure, Google Cloud
[12] Bspw. Atruvia, Finanzinformatik, Mambu
[13] Anbieter von Krypto-Dienstleistungen, Zentralverwahrer, zentrale Gegenparteien, Handelsplätze, Transaktionsregister, Verwalter alternativer Investmentfonds und Verwaltungsgesellschaften, Datenbereitstellungsdienste, Versicherungs- und Rückversicherungsunternehmen, Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, Einrichtungen der betrieblichen Altersversorgung (EbAV), Ratingagenturen, Abschlussprüfer und Prüfungsgesellschaften, Administratoren kritischer Referenzwerte, Crowdfunding-Dienstleister, Verbriefungsregister und IKT-Drittanbieter

eingestuft werden, so genannte „bedrohungsorientierte Penetrationstests“ durchführen (siehe Ausführungen zu Artikel 23).

Abbildung 3 zeigt zusammengefasst die wesentlichen Inhalte des Entwurfs der DORA[14].

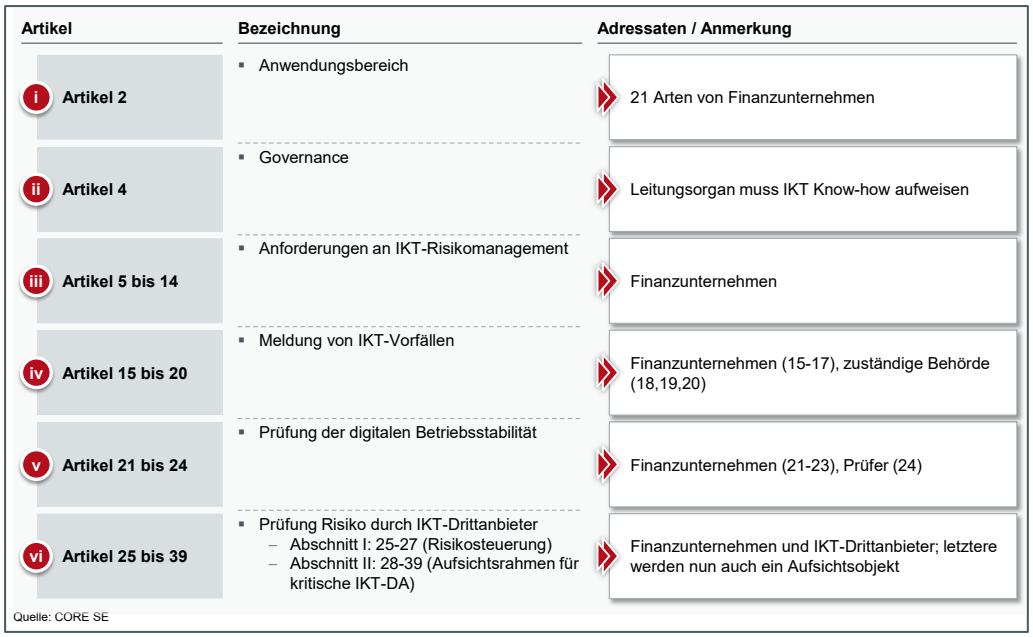


Abbildung 3: Themengebiete DORA nach Artikeln gruppiert

Governance (Artikel 4, Steuerung und Organisation)

DORA hebt die Bedeutung der IKT durch eine optimierte Abstimmung der Geschäftsstrategien von Finanzunternehmen mit dem IKT-Risikomanagement an. Zweckdienlich werden die Leitungsorgane der Aufsichtsobjekte eine entscheidende und aktivere Rolle bei der Steuerung des IKT-Risikomanagements übernehmen müssen. Es wird der Begriff der Cyberhygiene eingeführt, die durch die Leitungsorgane durchzusetzen ist. In letzter Konsequenz wird die Geschäftsleitung für die Steuerung von IKT-Risiken verantwortlich gemacht. Dies ist kein neuer Umstand, denn aus Sicht der Aufsicht ist das Wesen eines Finanzunternehmens das Management von Risiken, jedoch wird nun mit IKT-Risiken eine Risikoart exponiert.

Das Leitungsorgan ist vollständig über IKT-Risiken zu informieren. Finanzunternehmen überwachen IKT-Drittanbieter inklusive der damit verbundenen Risikoexposition. Zudem müssen die Mitglieder des Leitungsorgans regelmäßig Fachschulungen absolvieren, um ausreichende Kenntnisse und Fähigkeiten zu erwerben. Ebenso ist dieses Wissen aktuell zu halten, damit IKT-Risiken und deren Auswirkungen auf die Geschäftstätigkeit des Finanzunternehmens verstanden und bewertet werden können. Auf der Seite des Leitungsorgans wird die DORA zusammenfassend mehr MINT[15]-Expertise erzwingen. Diese Entwicklung wird sich in die Aufsichtsgremien fortschreiben.

[14] Version 24.9.2020, COM(2020) 595 final, 2020/0266 (COD)
[15] Mathematik, Informatik, Naturwissenschaft und Technik

IKT-Risikomanagement (Artikel 5 bis 14)

Die Anforderungen an das IKT-Risikomanagement orientieren sich an einschlägigen internationalen, nationalen und branchenspezifischen Normen, Leitlinien und Empfehlungen und betreffen spezifische Funktionen des IKT-Risikomanagements (Identifizierung, Schutz und Prävention, Erkennung, Gegenmaßnahmen und Wiederherstellung, Lernen sowie Weiterentwicklung und Kommunikation).

Diese 10 Artikel umfassen Themengebiete operativer Betriebssicherheit (hier „stabile IKT-Systeme und Instrumente“ genannt), welche Auswirkungen von IKT-Risiken minimiert, kontinuierlich Ursachen von IKT-Risiken ermittelt, Schutz- und Präventionsmaßnahmen ergreift, anormale Aktivitäten umgehend aufdeckt, Strategien für die Fortführung des Geschäftsbetriebs sowie Notfall- und Wiederherstellungspläne einrichtet. Ferner erstrecken sich diese Anforderungen auf die Sicherheit und Robustheit physischer Infrastrukturen und IKT-Drittanbieter von Finanzunternehmen.

Doch einige Anforderungen verdienen eine genauere Betrachtung:

> **Artikel 5 Absatz 4** (IKT-Risikomanagementrahmen) fordert die Anwendung eines „Systems für die Steuerung der Informationssicherheit“; somit wird die Einführung eines ISMS (**I**nformations**s**icherheits**m**anagement**s**ystem) eingefordert. Diese sind bereits regulatorisch durch die BAIT (Vorbemerkung 3) für Kreditinstitute resp. für Kapitalverwaltungsgesellschaften (Vorbemerkung 2 der KAIT), Versicherungen (Vorbemerkung 6 der VAIT) und für Zahlungs- und E-Geld-Institute (Vorbemerkung 3 der ZAIT) gefordert. Ein vollumfängliches ISMS ist in der Praxis selten implementiert. Diesem Umstand wird DORA durch die europäische Harmonisierung von IKT-Anforderungen begegnen , was der Durchsetzung von ISMS förderlich sein wird. Die Autoren postulieren, dass ein ISMS im Rahmen einer nächsten Regulierungsrunde in 3 bis 5 Jahren für wichtige Prozesse zertifiziert werden muss. Diese Entwicklung wird durch die geforderten bedrohungsorientierten Penetrationstests begünstigt, denn damit steigen die Anforderungen an den Schutz von Informationen und damit das Management der Schutzmaßnahmen.
>
> **Artikel 5 Absatz 9** fordert mit der „Strategie für digitale Resilienz“ die Erstellung einer Strategie und stellt gleichzeitig Vorgaben für deren Mindestinhalte auf. Die Strategie wird mit Indikatoren zur Messung und Überwachung der festgelegten strategischen Ziele auszustatten sein. Damit erfährt die IKT eine enorme Aufwertung im Vergleich zu bisherigen strategischen Zielen wie Geschäft in der Geschäftsstrategie, Auslagerung resp. Ausgliederung in der Outsourcing-Strategie und Risiken in der Risikostrategie. Eine resiliente IKT ist nun als gleichwertige notwendige Bedingung für das Geschäft des Finanzsektors anerkannt und muss in einer separaten Strategie behandelt werden. Im Lichte der IKT als bestimmenden Faktor im Finanzgeschäft ist das eine begrüßenswerte Entwicklung.

Artikel 5 Absatz 10 ermöglicht die Überprüfung der Einhaltung der Anforderungen an das IKT-Risikomanagement nach Genehmigung durch die zuständige Behörde[16] an Dritte zu delegieren. Dieser Absatz birgt eine zweifache Herausforderung:

- Erstens steigt der bürokratische Aufwand für Finanzunternehmen sowie die BaFin,
- zweitens können Finanzunternehmen unter Bedingungen eine sehr sensible 2nd LoD[17]-Funktion auslagern. Hier muss abgewartet werden wie sich das mit dem Verbot der Auslagerung der ISB-Funktion für Banken (BAIT II Tz. 4.6), Kapitalverwaltungsgesellschaften (KAIT Tz. 29), Versicherungen (VAIT II Tz. 4.7) und für Zahlungs- und E-Geld-Instituten (ZAIT II Tz. 4.6) sowie der Risikocontrolling-Funktion gemäß MaRisk AT 4.4.1 „verträgt".

Artikel 6 (IKT-Systeme, -Protokolle und -Instrumente) hebt gesamthaft auf die Anwendung des Standes der Technik ab und formuliert insofern keine neuen Anforderungen. Jedoch kann der Begriff „technologisch stabil" (Absatz 1 lit. d) als unscharf formuliert angesehen werden. Unter Beachtung der Ausführungen in Artikel 6 als „Beachtung stabiler Lieferketten" gedeutet, da nicht nur das Schutzziel Verfügbarkeit, auch die Schutzziele Authentizität und Integrität (bei Software) adressiert werden, dürfte der Regelungsraum und das einhergehende Rational hinreichend exakt beschrieben sein.

Artikel 7 (Identifizierung) fordert mit detaillierten Ausführungen eine Strukturanalyse/ Prozesslandkarte (Absatz 1), ein Risikomanagement (Absatz 2), Risikoanalysen bei jeder wesentlichen Änderung (Absatz 3), die Kenntnis aller Ressourcen, teilweise in Verzeichnissen (Absatz 6), wie Konten, Netze, Hardware, kritische physische Ausrüstung, Konfigurationen, Verbindungen und Interdependenzen (in Absatz 4) und der Prozesse bei IKT-Drittanbietern (in Absatz 5). Absatz 7 fordert die regelmäßige Bewertung des IKT-Risikos von IKT-Altsystemen, ohne den Begriff „IKT-Altsysteme" näher zu beschreiben. Die Forderung nach Kenntnis aller Ressourcen aus Absatz 4 und 5 sollten Finanzunternehmen bereits im Rahmen der Strukturanalyse/Prozesslandkarte (Absatz 1) erfüllen.

Artikel 8 (Schutz und Prävention) fordert die Überwachung und Kontrolle der Funktionsweise der IKT-Systeme und -Instrumente (in Absatz 1), die Gewährleistung von Resilienz, Kontinuität und Verfügbarkeit von IKT-Systemen sowie die CIA[18]-Schutzziele der Daten in der kompletten Verarbeitungskette - Speicherung, Verwendung und Übermittlung (in Absatz 2), den Einsatz von Kryptographie (in Absatz 3), eine „Policy für Informationssicherheit" zur Erreichung der CIA-Schutzziele (in Absatz 4 lit. a), ein mit dem Need-to-know-Prinzip arbeitendes Identity Access Management (in Absatz 4 lit. c), den Schutz von kryptografischen Schlüsseln (in Absatz 4 lit. d), ein Änderungsmanagement (in Absatz 4 lit. e) und eine Strategie für Patches und Updates. Hinzu kommen noch die

[16] die nationalen Aufsichtsbehörden, in Deutschland BaFin und Bundesbank
[17] Line of Defence
[18] C= confidentiality (Vertraulichkeit), I=integrity (Integrität), A=authenticity (Authentizität)

Netzwerksegmentierung und ein Änderungsmanagement für den Notfall inklusive Berichtslinien. Die o.g. „Policy für Informationssicherheit“ adressiert das klassische Management von Vermögenswerten (‚asset management‘) im Rahmen der Themen „Informationsklassifizierung“ und „Informationskennzeichnung“ (‚labeling‘); dieses muss um den Schutz der Informationen entlang ihres Lebenszyklus und der sie verarbeitenden Anwendungen und Systeme ergänzt werden, am besten durch ein IT-Betriebshandbuch.

Artikel 9 (Erkennung) widmet sich der Erkennung von Anomalien bei der Leistungserbringung von IKT-Netzen und von IKT-Vorfällen. Die Fähigkeit zur Erkennung muss mit angemessenen Ressourcen und Kapazitäten ausgestattet sein. Speziell Kreditinstituten wird mit der Anomalienerkennung von Handelsauskünften eine besondere Anforderung zuteil (in Absatz 4).

Artikel 10 (Gegenmaßnahmen und Wiederherstellung) führt in Absatz 1 eine „IKT-Strategie zur Fortführung des Geschäftsbetriebes“ ein und detailliert diese in den Inhalten in Absatz 2 als Mischung aus Incident Management und Business Continuity Management aus. Absatz 3 führt einen „IKT-Plan für die Wiederherstellung im Notfall" ein, der einer unabhängigen Prüfung zu unterziehen ist. Gemeint ist ein IKT-Plan für den IKT-Risikomanagementrahmen aus Artikel 5 Absatz 1, d.h. das „Management von Risiken“ und ein „hohes Maß an digitaler Betriebsstabilität“. Im Klartext muss der Risikomanagementprozess mindestens durch die Interne Revision überprüft werden. Auch die Jahresabschlussprüfung ist eine geeignete Prüfung. Die Prüfung der „digitalen Betriebsstabilität“ kann am besten durch eins der großen zwei neuen Themen der DORA realisiert werden: die bedrohungsorientierten Penetrationstests (siehe Ausführungen zu Artikel 23).

Absatz 4 leitet zu Plänen zur Fortführung des Geschäftsbetriebes über. Diese müssen zusammen mit den Kommunikationsplänen gemäß Absatz 5 mindestens jährlich überprüft werden. Es folgen die Verpflichtungen eine Krisenkommunikationsfunktion (Absatz 6) festzulegen, Aufzeichnungen zu Störungen anzufertigen (Absatz 7), die Anforderung speziell an Zentralverwahrer Testergebnisse an die Aufsicht zu übermitteln (Absatz 8) und wiederum an alle Finanzunternehmen Kosten und Verluste aus IKT-Vorfällen an die zuständige Behörde zu melden (Absatz 9). Kurzum: Finanzunternehmen müssen ein Business Continuity Management System (BCMS) einführen. Dieses sollten sie nach Ansicht der Autoren mit Hilfe des BSI-Standards 200-4 angehen. Auch zu diesem Absatz eine Anmerkung: Was macht die zuständige Behörde mit den gemeldeten Kosten und Verlusten? Diese Datenbank ist ein lohnendes Ziel für die Organisierte Kriminalität und somit ein exponiertes Angriffsziel.

Artikel 11 widmet sich den „Strategien für Datensicherung und Wiederherstellungsverfahren“ und legt Zentralen Gegenparteien (Absatz 3) und Zentralverwahrern (Absatz 4) besondere Pflichten bei den Wiederherstellungsplänen resp. dem sekundären Bearbeitungsstandort (Absatz 5) auf.

Artikel 12 behandelt „Lernprozesse und Weiterentwicklung“ nach IKT-Vorfällen und verpflichtet in Absatz 2 Finanzunternehmen zur Meldung von Änderungen an die zuständigen Behörden. Hierbei werden allerdings keine Kriterien für die Meldung genannt.

Artikel 13 „Kommunikation“ birgt keine Überraschungen und verpflichtet Finanzunternehmen über Kommunikationspläne zu verfügen (Absatz 1), welche zwischen internen und externen Empfängern unterscheiden, wobei die internen weiter unterteilt werden in Wissende zum IKT-Risikomanagement und allen anderen Personen sowie der Beauftragung von mindestens einer Person als Umsetzer der Kommunikationsstrategie und als Sprecher nach extern.

Artikel 14 (Weitere Harmonisierung von Instrumenten, Methoden, Prozessen und Strategien für IKT-Risikomanagement) führt zum ersten Mal „Technische Regulierungsstandard“ (RTS) ein, welche die ESA in Kooperation mit der ENISA erarbeiten sollen. Diese sollen die in Artikeln 8, 9 und 10 benannten Strategien, Verfahren, Protokolle, Instrumente, Komponenten, Prüfungen und Elemente für IKT-Sicherheit weiter detaillieren.

Eine Zusammenstellung aller zu erstellender RTS und ITS aus DORA findet sich in Abbildung 4.

RTS ITS

Artikel	Thema RTS / ITS	Frist Bezug Inkrafttreten
14a)	▪ 8(2): CIA-Schutz von Daten und Systemen	1 Jahr nach
14b)	▪ 8(2): Security by Design, Threat Management	1 Jahr nach
14c)	▪ 8(4) lit. b: Netz- und Infrastrukturmanagement inkl. Isolierung betroffener Informationsressourcen im Falle von Cyberangriffen	1 Jahr nach
14d)	▪ 8(4) lit. c: Rollen- und Rechtemanagement inkl. Zutritts- und Zugangsschutz	1 Jahr nach
14e)	▪ 9(1) (2): Erkennung IKT -bezogener Vorfälle, SIEM, SOC	1 Jahr nach
14f)	▪ 10(1): IKT-Plan für Fortführung des Geschäftsbetriebs als Bestandteil der operativen Strategie zur Fortführung des Geschäftsbetriebs	1 Jahr nach
14g)	▪ 10(5): Jährliche Überprüfung des IKT -Plans für die Wiederherstellung im Notfall sowie für die Fortführung des Geschäftsbetriebs	1 Jahr nach
14h)	▪ 10(3): Komponenten des IKT -Plans für Wiederherstellung im Notfall, der einer unabhängigen Prüfung zu unterziehen ist	1 Jahr nach
16(3)	▪ 16(2) lit. a: Kriterien für Bestimmung schwerwiegender IKT -Vorfälle mit Meldepflicht	1 Jahr nach
16(3)	▪ 16(2) lit. b: Kriterien zur Bedeutung der Relevanz schwerwiegender IKT -Vorfälle in anderen Ländern	1 Jahr nach
18(1) lit. a	▪ Inhalt von Berichten über schwerwiegende IKT - Vorfälle + Bedingungen zur Delegation der Melde - pflicht (mit Genehmigung der zuständigen Behörde)	1 Jahr nach

Artikel	Thema RTS / ITS	Frist Bezug Inkrafttreten
18(1) lit. b	▪ Standartformulare, Vorlagen und Verfahren zur Meldung eines schwerwiegenden IKT -Vorfalles	1 Jahr nach
19(1)	▪ Bericht zur Prüfung einer EU -Plattform für schwerwiegende IKT -Vorfälle	3 Jahre nach
23(4)	▪ Details zu intelligenzgestützten Penetrationstests	2 Monate vor
25(10)	▪ Standardvorlage für Informationsregister zu Verträgen mit IKT -Drittanbietern	1 Jahr nach
25(11) lit. a, b	▪ a) Richtlinie zur Nutzung von IKT -Diensten ▪ b) Informationsarten für Informationsregister zu Verträgen mit IKT -Drittanbietern	1 Jahr nach
27(4)	▪ (2) lit. a Beschreibung aller Funktionen und Dienstleistungen, die der IKT -Drittanbieter zu erbringen hat inkl. Zulässigkeit für Untervergaben	1 Jahr nach
35(3)	▪ Ernennung Mitglieder des gemeinsamen Unter - suchungsteams; Aufgaben und Arbeitsanweisungen	1 Jahr nach
36(1) lit. a	▪ Informationen für freiwilligen Antrag des IKT - Drittanbieters	1 Jahr nach
36(1) lit. b	▪ aus 31(1): Inhalt und Format für Abschlussberichte zur Umsetzung von Maßnahmen	1 Jahr nach
36(1) lit. c	▪ aus 31(1): Informationen, inkl. Struktur, Formaten und Methoden, die ein IKT -Drittanbieter vorlegen muss	1 Jahr nach
36(1) lit. d	▪ aus 37(2): Bewertung der Maßnahmen der IKT - Drittanbieter zu Empfehlungen der federführenden Aufsichtsinstanz	1 Jahr nach

Abbildung 4: aus DORA resultierende Regulatory Technical Standards (RTS) und Implementing Technical Standards (ITS)

Meldung IKT-bezogener Vorfälle (Artikel 15 bis 20)

Das Meldewesen wurde ergänzt. In nachfolgenden sechs Artikel werden die Anforderungen an Meldungen von IKT-Vorfällen detailliert:

Artikel 15 legt Finanzunternehmen eine „Vorgehensweise für die Bewältigung IKT-bezogener Vorfälle“ auf. Diese muss u.a. die Aspekte integrierte Überwachung, Handhabung und Weiterverfolgung von IKT-Vorfällen, ihre Verfolgung, Protokollierung, Kategorisierung und Klassifizierung entsprechend Schwere und Kritikalität, bis hin zu Kommunikationsplänen für intern/extern und einem Meldewesen enthalten. Diese

Themenstellung zum Management von Sicherheitsvorfällen wird in einem ISMS üblicherweise im gleichnamigen Segment bearbeitet.

Artikel 16 (Klassifizierung IKT-bezogener Vorfälle) stellt auf Klassifizierungskriterien IKT-bezogener Vorfälle ab: diese sind Zahl betroffener Nutzer, Dauer, geografische Ausbreitung, Datenverluste, Schwere der Auswirkungen, Kritikalität betroffener Dienste und wirtschaftliche Auswirkungen. Auch werden aus diesem Artikel zwei RTS[19] erstellt (siehe Abbildung 4).

Artikel 17 verpflichtet alle Adressaten der DORA zur Meldung schwerwiegender IKT-Vorfälle; bisher galt das nur für KRITIS-Unternehmen und KRITIS-Systeme. Des Weiteren formuliert der Artikel viele Details zum Meldewesen wie z.B. Fristen für die „Meldung schwerwiegender IKT-bezogener Vorfälle“ an die zuständige Behörde (Abs. 3 lit. a) – unterteilt in Erstmeldung, Zwischenberichte und Abschlussbericht. Eine Delegation von Meldepflichten ist nur mit Genehmigung der zuständigen Behörde möglich, was eine bürokratische Hürde darstellt. Die zuständige Behörde informiert die sachgerechte ESA-Behörde, bei Finanzunternehmen auch die EZB, sowie die so genannte „zentrale Anlaufstelle“ gemäß der NIS-Richtlinie - in Deutschland das BSI.

Artikel 18 (Harmonisierung von Inhalt und Vorlagen von Meldungen) gemäß dieses Artikels erarbeiten ESA[20], ENISA und EZB ein ITS zu Inhalt von Berichten über schwerwiegende IKT-Vorfälle und die Bedingungen zur Delegation der Meldepflichten an Dritte.

Artikel 19 (Zentralisierung Berichterstattung über schwerwiegende IKT-Vorfälle) beschreibt die Aufgabe für ESA, EZB[21] und ENISA[22], einen Bericht zur Prüfung der Einrichtung einer einheitlichen EU-Plattform für die Meldung schwerwiegender IKT-Vorfälle zu erstellen. Der Bericht soll an das Europäische Parlament und den Rat 3 Jahre nach Inkrafttreten von DORA übermittelt werden. Mit dieser zentralisierten Meldeplattform taten sich schon die deutschen KRITIS-Betreiber zu Zeiten des UP KRITIS[23] und des IT-SiG 1.0 in den Jahren 2008 bis 2015 schwer; es bleibt somit abzuwarten, wie dieses Vorhaben auf europäischer Ebene aufgegriffen wird, denn diese zentrale Datenbank stellt ein hoch motivierendes Ziel für Angriffe dar.

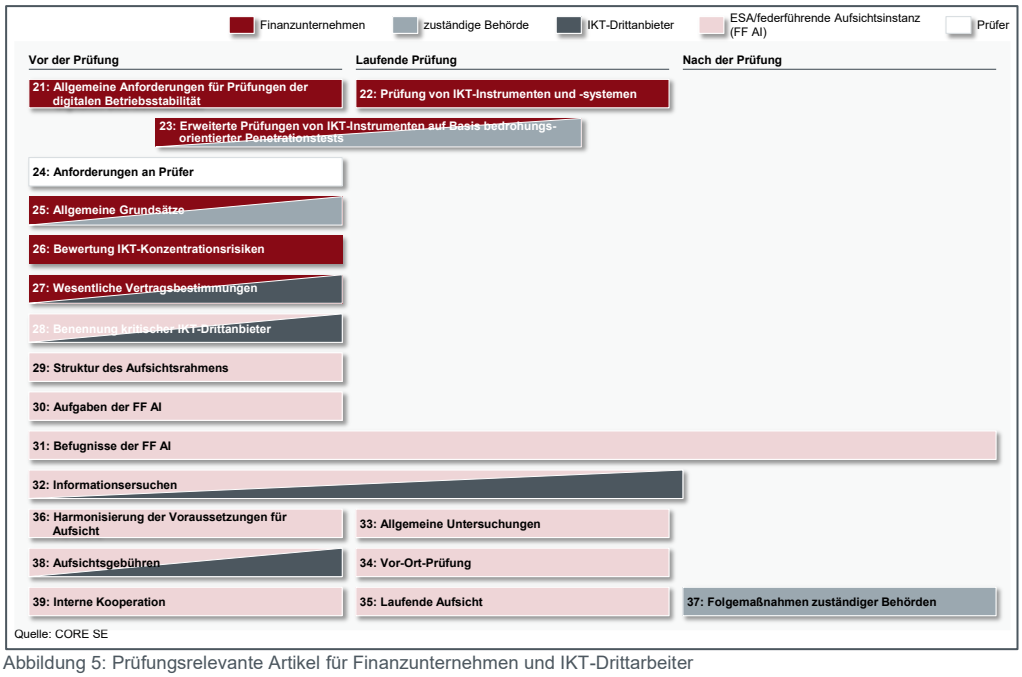
[19] RTS=Regulatory Technical Standard (Detailierte techische Anforderungen aus einem europäischen Regulierungswerk)
[20] ESA=European Supervisory Authorities (Die drei europäischen Aufsichtsbehörden im Finanzsektor: die Europäische Bankenaufsichtsbehörde (European Banking Authority [EBA]), die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersvorsorge (European Insurance and Occupational Pensions Authority [EIOPA]) sowie die Europäische Wertpapier- und Marktaufsichtsbehörde (European Securities and Markets Authority [ESMA])
[21] EZB=Europäische Zentralbank
[22] ENISA= European Network and Information Security Agency (Agentur der Europäischen Union für Cybersicherheit)
[23] Umsetzungsplan Kritische IT-Infrastrukturen

Prüfung der digitalen Betriebsstabilität - Artikel 21-24

Kapitel IV (Artikel 21 bis 24) und Kapitel V (Artikel 25 bis 39) bilden die prüfungsrelevanten Artikel und sie spannen den Rahmen für die Prüfung der IKT bei Finanzunternehmen allgemein und IKT-Drittanbietern im Speziellen weit auf.

Kapitel IV stellt mit den Artikeln 21 bis 24 die Prüfung der digitalen Betriebsstabilität dar. Neu und damit besonders erwähnenswert zu **Artikel 21** (Allgemeine Anforderungen für Prüfungen der digitalen Betriebsstabilität) ist die Etablierung eines Programms zur jährlichen Prüfung der digitalen Betriebsstabilität aller kritischen IKT-Systeme und -Anwendungen; dieses umfasst Inhalte aus den Artikeln 22 und 23 und eine Risiko-gesteuerte Prüfung der Betriebsstabilität inklusive der Mitigation aller Feststellungen.

Die Beschreibung des Geltungsbereichs als „digitale Betriebsstabilität“ umfasst alle Anwendungen, Komponenten, Systeme und Informationen und ist in diesem Umfang neu. Bisher reduziert die Regulierung die Aufwände durch Ausdrücke wie „wesentliche Auslagerungen“, „kritische Systeme“ oder auch „wichtige Systeme“. Nun muss das Finanzunternehmen vollumfänglich digital betriebsstabil sein.



Quelle: CORE SE

Abbildung 5: Prüfungsrelevante Artikel für Finanzunternehmen und IKT-Drittarbeiter

Artikel 22 (Prüfung von IKT-Instrumenten und -Systemen) gibt durchzuführende Tests gemäß Artikel 21 vor und eröffnet eine Vielzahl an Anforderungen an Analysen, Überprüfungen und Bewertungen. Speziell Zentralverwahrer und Zentrale Gegenparteien müssen die Anfälligkeit von Änderungen an kritischen Funktionen, Anwendungen und Infrastrukturkomponenten bewerten.

Nach **Artikel 23** (Erweiterte Prüfungen von IKT-Instrumenten, -Systemen und -Prozessen auf Basis bedrohungsorientierter Penetrationstests) müssen kritische Finanzunternehmen (Festlegung welche kritisch sind siehe Artikel 23 Absatz 3) alle 3 Jahre bedrohungsorientierte Penetrationstests durchführen. Diese Penetrationstests umfassen zumindest kritische Funktionen, auch die ausgelagerten, und werden an Live-Produktionssystemen durchgeführt. Die zuständige

Behörde muss den Umfang des Penetrationstests genehmigen und nach Durchführung auch die ordnungsgemäße Durchführung bescheinigen.

Die zuständige Behörde ermittelt Finanzunternehmen, die bedrohungsorientierte Penetrationstests durchzuführen haben mit Hilfe der Faktoren aus Absatz 3. ESA und EZB erstellen zusammen ein RTS für „intelligenzgestützte“ Penetrationstests zu den Aspekten

- Umfang der bedrohungsorientierten Penetrationstests,
- Prüfmethodik und Prüfkonzept, Finalisierung der Prüfungen sowie
- der Art der aufsichtlichen Zusammenarbeit bei Finanzunternehmen, die in mehreren Mitgliedsstaaten tätig sind

Mit der Einholung der Genehmigung des vorgesehenen Penetrationstests bei der BaFin kommt weiterer neuer Verwaltungsaufwand auf Finanzunternehmen zu. Auch die BaFin muss ob der Zahl der neu hinzukommenden Aufsichtsobjekte sowie der Vielzahl erweiterter IT-fachlicher Anforderungen weitere Kapazitäten aufbauen.

Eine weitere Herausforderung ist die Anforderung Penetrationstests im Produktivsystem durchzuführen, da dies verschiedene Risiken birgt (siehe Kasten „Risiken von Penetrationstests in Live-Umgebung“). Hier plädieren die Autoren für Penetrationstests in Staging-Umgebungen und der Begründung der Vergleichbarkeit zu einem Penetrationstest in der Live-Umgebung in Form einer Risikoanalyse.

Risiken von Penetrationstests in Live-Umgebung

Beeinträchtigung der Finanzmarktstabilität: Wie reagiert die Aufsicht bei schwerwiegenden Ausfällen in Folge eines erfolgreichen Penetrationstests? Hier kollidieren die Aufsichtsziele „Finanzmarktstabilität", „Management von Risiken" sowie „Penetrationstest in Live-Umgebung" und bergen ein Dilemma für Finanzunternehmen. Schließlich kann aus BAIT II Tz. 8.5 abgeleitet werden, dass Penetrationstests in Produktivsystemen verboten sind.

Störung der Kunden: Da externe Penetrationstests dazu dienen, die Sicherheit der externen Schnittstellen (Internet) zur Umgebung des Finanzunternehmens zu bewerten, besteht bei Tests in der Produktionsumgebung ein größeres Risiko, dass der tägliche Geschäftsbetrieb und die Kunden beeinträchtigt werden, selbst wenn es nur zu einer geringfügigen Störung der Systeme kommt. Je nach Anwendungsfall des Ziels und dem Ausmaß der Unterbrechung können die Auswirkungen erheblich sein.

Vertraulichkeit, Integrität/Authentizität und Verfügbarkeit von Daten: Da es sich bei Daten in der Produktion um reale Kundendaten handelt, die streng vertraulich sind, besteht während der Tests das Risiko, dass Daten für Dritte offengelegt und manipuliert werden. Zudem besteht die Gefahr System- und Serviceausfälle zu provozieren, die die Vertraulichkeit, Integrität/Authentizität und Verfügbarkeit beeinträchtigen.

Zeit und Umfang: Planung und Durchführung von Tests in einer Produktionsumgebung sind in der Regel zeitaufwändig, da Umfang, Ziel des Tests und die zu verwendenden Methoden klar definiert und verstanden werden müssen. Sobald der Umfang festgelegt ist, realisieren externe Penetrationstester Tests sorgfältig und versuchen, die Integrität und Verfügbarkeit der Kundendaten und -systeme nicht absichtlich zu beeinträchtigen. Diese Art von Tests konsumiert erheblich mehr Ressourcen und kann trotzdem zu Serviceunterbrechungen führen sowie Kunden beeinträchtigen. Das Ergebnis ist eine geringere Testabdeckung innerhalb der begrenzten Testfenster.

Informationsverschmutzung: Um Schwachstellen (falls vorhanden) zu identifizieren, verwenden Penetrationstester Manipulationstechniken, die dazu führen können, dass Daten aufgedeckt, verändert und bösartiger Code, Skripte, SQL-Anweisungen usw. in das Netzwerk oder die Anwendung injiziert werden. Dies führt zu einer Vielzahl bösartiger Daten und Einstellungen in der Produktionsumgebung als Zielsystem des Penetrationstests. Eine wirksame manuelle Bereinigung ist nicht immer vollständig möglich.

Artikel 24 (Anforderungen an Prüfer) definiert die Bedingungen an Prüfer für bedrohungsorientierte Penetrationstests. So müssen sie durch eine Akkreditierungsstelle zertifiziert sein oder sich an formale Verhaltenskodizes oder ethische Rahmenregelungen halten. Externe Prüfer müssen zudem eine unabhängige Gewähr oder ein Bestätigungsvermerk für zuverlässige Steuerung von Risiken inkl. Schutz vertraulicher Informationen und einen Versicherungsschutz (Berufshaftpflicht und gegen Fehlverhalten/Fahrlässigkeit) nachweisen.

Geklärt werden muss welche Verhaltenskodizes und ethische Rahmenregelungen den Anforderungen genügen und welche Institution die Einhaltung testieren darf. Gleiches gilt für die Gewähr und den Bestätigungsvermerk. Zu vermeiden gilt, dass im Zweifel formale Kriterien mit neuen verwaltungstechnischen Hürden vor gewachsenen vertrauensvollen Geschäftsbeziehungen zwischen Finanzunternehmen und Penetrationstestern gelten.

Steuerung des Risikos durch IKT-Drittanbieter - Artikel 25-39

Das große Kapitel V zu IKT-Drittanbietern besteht aus den 15 Artikeln 25 bis 39 und ist in zwei Abschnitte unterteilt – Abschnitt I (Grundsätze für eine zuverlässige Steuerung des Risikos durch IKT-Drittanbieter) mit den Artikeln 25 bis 27 und Abschnitt II (Aufsichtsrahmen für kritische IKT-Drittanbieter) mit den Artikeln 28 bis 39 – siehe Abbildung 5.

Artikel 25 (Allgemeine Grundsätze) spannt den Rahmen der Risikosteuerung durch IKT-Drittanbieter auf und fordert in Absatz 3 die Entwicklung einer „Strategie für das Risiko durch IKT-Drittanbieter“ als Teil des IKT-Managementrahmens. Diese muss u.a. ein Register zu Verträgen mit IKT-Drittanbietern enthalten. Ferner unterrichten IKT-Drittanbieter die zuständige Behörde über die geplante Vergabe von Aufträgen für kritische oder wichtige Funktionen (auch nachträglich bei Hochstufung einer Funktion), was in Deutschland bereits das FISG fordert. Unter anderem müssen Finanzunternehmen die Erhöhung des IKT-Konzentrationsrisikos (siehe Ausführungen zu Artikel 26 weiter unten) bewerten. Absatz 9 fordert neben umfassenden und dokumentierten Ausstiegsszenarien „gegebenenfalls“ auch deren „ausreichende“ Erprobung. Hier besteht Klärungsbedarf: wann müssen Finanzunternehmen Ausstiegsszenarien und in welcher Form prüfen? Reicht eine Planbesprechung oder muss es ein Funktionstest sein? Zur Präzisierung sollte festgestellt werden, dass XAIT (BAIT / KAIT / VAIT / ZAIT) keine Anforderung der vollständigen Test-Übertragung und Test-Inbetriebnahme der gesamten IT-Systemlandschaft von einem Dienstleister zu einem zweiten Dienstleister stellt.

Artikel 26 (Vorläufige Bewertung des IKT-Konzentrationsrisikos und weiterer Vereinbarungen über weiteres Outsourcing) legt Finanzunternehmen weitere neue Bewertungs- und Entscheidungspflichten auf. Bei der Ermittlung des IKT-Konzentrationsrisikos müssen sie berücksichtigen, ob sie IKT-Drittanbieter nutzen die „nicht ohne Weiteres ersetzbar sind“ oder „mehrfach vertragliche Vereinbarungen mit demselben/eng verbundenen IKT-Drittanbieter“ schließen. Hierbei müssen Finanzunternehmen Alternativen untersuchen. Auch müssen sie die Risiken bei Auslagerung von wichtigen Funktionen durch IKT-Drittanbieter an Unterauftragnehmer bewerten. Das ist bereits aus der Datenschutzregulierung bekannt, findet jetzt aber Eingang in die europäische Finanz-Regulierung.

Schließlich dürfen Finanzunternehmen mit einem IKT-Drittanbieter aus einem Drittland nur dann einen Vertrag schließen, wenn die Einhaltung des Datenschutzes und die wirksame Durchsetzung des Rechts gewährleistet sind. Diese Forderungen entspringen der Rechtsprechung des EuGH zum Privacy Shield vom 16.07.2020 – besser als Schrems II bekannt – und suggerieren, dass diese Problematik bei IKT-Drittanbietern in Europa gelöst sei. Dem ist nicht so: die Verarbeitung von personenbezogenen Daten in Hyperscalern US-amerikanischer Provenienz – in den USA oder in Europa als Tochter eines US-amerikanischen Unternehmens – ist derzeit nicht konform zur DSGVO möglich, denn hierzu müsste das europäische auslagernde Unternehmen beweisen, dass die USA ein dem europäischen vergleichbares Datenschutzniveau aufweisen. Diesen Beweis kann das europäische Unternehmen regelmäßig nicht führen.

Bedeutsam ist ferner die Anforderung, Ketten von Unterauftragnehmern hinsichtlich Überwachbarkeit durch das Finanzunternehmen selbst als auch die zuständige Behörde zu evaluieren. Hierzu müssen die Finanzunternehmen genaue Kenntnisse zu den Fähigkeiten der zuständigen Behörden erlangen, um „mitzugestalten“ können. Dazu sollte es ebenfalls einen „Gemeinsamen Ausschuss“ (analog zum gleichnamigen Ausschuss der ESA) aus Finanzunternehmen und BaFin geben; es böte sich das weiter zu entwickelnde „Fachgremium IT“ der BaFin an.

Artikel 27 (Wesentliche Vertragsbestimmungen) beschreibt im Detail die Mindestinhalte des Vertrages zwischen Finanzunternehmen und IKT-Drittanbieter. Erwähnenswert aus dem Entwurf ist ein Detail aus Absatz 2 Buchstabe j, wonach die Kündigungsrechte und die damit zusammenhängenden Mindestkündigungsfristen „den Erwartungen der zuständigen Behörden“ entsprechen müssen. Dazu sollten diese Erwartungen den Finanzunternehmen vorher bekannt sein – Stichwort „Fachgremium IT“. Wenn vorhanden, sollen gemäß Absatz 3 Finanzunternehmen und IKT-Drittanbieter Standardvertragsklauseln verwenden. Auch aus diesem Artikel heraus wird ein RTS entstehen, das gemäß Absatz 2 Buchstabe a eine klare und vollständige Beschreibung aller Funktionen und Dienstleistungen, die der IKT-Drittanbieter zu erbringen hat, vornimmt. Es bleibt abzuwarten, ob und wie sich die Aufsicht der IKT-Drittanbieter auf die Bereitschaft beispielsweise der Hyperscaler auswirkt, mehr auf die Vorstellungen und Wünsche der Finanzunternehmen einzugehen. Bisher liegt die Verhandlungsmacht trotz Moderation der Regulation bei den Hyperscalern.

Zentral für die DORA ist **Artikel 28** mit den Regelungen zur „Benennung kritischer IKT-Drittanbieter“. Vereint ein IKT-Drittanbieter eine bestimmte Höhe an Vermögenswerten von Finanzunternehmen, die ihn nutzen, stellt die ESA (und nicht die nationale zuständige Behörde) die „federführende Aufsichtsinstanz“ des IKT-Drittanbieters. Im „Gemeinsamen Ausschuss“ (die Zusammenarbeit von EBA, EIOPA und ESA im Rahmen der ESA an DORA) benennt die ESA IKT-Drittanbieter unter Beachtung der Kriterien aus Absatz 2. Besondere Erwähnung bedarf die „systematische Auswirkung auf Stabilität, Kontinuität oder Qualität der Erbringung der Finanz-Dienstleistungen bei Betriebsstörung des IKT-Drittanbieters“. Wobei die Zahl der Finanzunternehmen zu berücksichtigen ist, für die der IKT-Drittanbieter Dienstleistungen erbringt. Hier muss darauf hingewiesen werden, dass Hyperscaler mit der technisch gesehen unlimitierten Skalierbarkeit und der weltweit verteilten Verfügbarkeit durch „Availability Zones“ diesen Risiken wirkungsvoll begegnen. Der in den Buchstaben b) und c) des Absatzes 2 formulierte Mechanismus aus

„systemrelevanten Instituten“ (G-SRI) sowie „anderer systemrelevanter Institute“ (A-SRI) in ihrer Nutzung von IKT-Drittanbietern soll ebenfalls bei der Benennung kritischer IKT-Drittanbieter berücksichtigt werden. Gleiches gilt für die Wechselbeziehung untereinander und im restlichen Finanzsektor.

Es kann hinterfragt werden, wie die ESA dies bewerkstelligen und dabei die Balance aus freiem Wettbewerb, Wettbewerbsbeschränkungen und technologische Übersicht behalten will. Buchstabe d thematisiert den Grad der Substituierbarkeit des IKT-Drittanbieters: hier wäre eine Entwicklung ungünstig, nach der die ersten Hyperscaler nutzende Finanzunternehmen diese weiter nutzen dürfen, Finanzunternehmen die später Hyperscaler nutzen wollen dies wegen zu hoher Marktanteile der IKT-Drittanbieter nicht mehr dürfen. Nach Absatz 8 können IKT-Drittanbieter die Aufnahme in die Liste kritischer IKT-Drittanbieter beantragen. Denn nicht gelistete IKT-Drittanbieter werden es schwer am Markt haben. Nach Absatz 9 dürfen Finanzunternehmen einen in einem Drittland ansässigen IKT-Drittanbieter jedoch nicht nutzen, wenn er in der Europäischen Union als kritisch eingestuft würde. Hier stellt sich die Frage, woher die Finanzunternehmen wissen sollen, ob dieser Drittland-IKT-Drittanbieter in der Union in diese Blacklist aufgenommen wurde. Dazu müssen Finanzunternehmen diese Benennung durch die ESA simulieren können, d.h. ein verlässliches Bewertungssystem der ESA nutzen.

Artikel 29 (Struktur des Aufsichtsrahmens) birgt ein interessantes Detail im vierten Absatz: Das „Aufsichtsforum“ (ein Unterausschuss der ESA, der vorbereitende Arbeiten für Einzelentscheidungen und gemeinsame Empfehlungen für kritische IKT-Drittanbieter durchführt) legt umfassende Benchmarks kritischer IKT-Drittanbieter vor. Was bedeutet diese Aussage konkret? Erstellt die ESA eine „Best-of-Liste“ von IKT-Drittanbietern mit den besten Benchmarks? Was würde das für weniger performante IKT-Drittanbieter bedeuten?

Die „Aufgaben der federführenden Aufsichtsinstanz“ im **Artikel 30** bergen keine Überraschungen bei der Bewertung der Qualität der Steuerung der IKT-Risiken durch die IKT-Drittanbieter als ihre Hauptaufgabe. In Absatz 3 ist der Anspruch der federführenden Aufsichtsinstanz niedergeschrieben, die kritischen IKT-Drittanbieter mit Hilfe eines jährlich aktualisierten Plans zu beaufsichtigen. Die zuständige Behörde (in Deutschland die BaFin) darf nur in Absprache mit der federführenden Aufsichtsinstanz Maßnahmen beim IKT-Drittanbieter ergreifen. Das stellt eine bisher nicht normierte Machtteilung zwischen nationalen Aufsichten und der europäischen ESA dar. Heute kann die BaFin autonom agieren. **Artikel 31** regelt die „Befugnisse der federführenden Aufsichtsinstanz“: Diese kann alle benötigten Informationen und Unterlagen vom IKT-Drittanbieter anfordern, Untersuchungen durchführen, die ergriffenen Mitigationsmaßnahmen überprüfen und Empfehlungen zu allen Inhalten des Artikel 30 Absatz 2 abgeben. Diese „Empfehlungen“ sind als Auflagen zu verstehen und also mandatorisch umzusetzen. Unter anderem kann die federführende Aufsichtsinstanz die Nutzung eines Drittland-IKT-Drittanbieters für kritische oder wichtige Funktionen des Finanzunternehmens untersagen. Für die Bekanntheit des Artikels wird die Möglichkeit der Verhängung eines Zwangsgeldes bei Zuwiderhandlung zu Absatz 1 Buchstaben a bis c sorgen, d.h. wenn der IKT-Drittanbieter bei der Untersuchung nicht kooperiert. Gemäß Absatz 8 kann die ESA die Zwangsgelder unter Bedingungen veröffentlichen.

Die weiteren drei Artikel detaillieren die Befugnisse der federführenden Aufsichtsinstanz aus Artikel 31 Absatz 1 Buchstaben a und b aus:

- Artikel 32 „Informationsersuchen“ (gemäß Artikel 1 Buchstabe a)
- Artikel 33 „Allgemeine Untersuchungen“ (gemäß Artikel 1 Buchstabe b Stichwort „Untersuchungen“)
- Artikel 34 „Vor-Ort-Prüfungen“ (gemäß Artikel 1 Buchstabe b Stichwort „Inspektionen“)

Zu **Artikel 33** ist anzumerken, dass sich die Befugnisse der federführenden Aufsichtsinstanz wie eine polizeiliche Vorladung lesen, inklusive der Aushändigung von Aufzeichnungen von Telefongesprächen. Artikel 35 (Laufende Aufsicht) führt ein „gemeinsames Untersuchungsteam“ ein. So ein Team wird für jeden kritischen IKT-Drittanbieter eingerichtet und es besteht aus maximal 10 Mitgliedern gespeist aus federführender Aufsichtsinstanz und der zuständigen Behörde. Alle Mitglieder müssen über Fachwissen in den Bereichen IKT und operationellen Risiken verfügen, koordiniert wird das Team durch einen Mitarbeitenden der ESA. Die ESA wird einen RTS über die Ernennung der Mitglieder des gemeinsamen Untersuchungsteams sowie die Aufgaben und die Arbeitsvereinbarungen des Untersuchungsteams entwickeln. Gemäß Absatz 4 übermittelt die federführende Aufsichtsinstanz binnen 3 Monaten nach Untersuchungsabschluss Empfehlungen an den kritischen IKT-Drittanbieter und die zuständigen Behörden. Artikel 36 dient der „Harmonisierung der Voraussetzungen für die Durchführung der Aufsicht“ und verpflichtet die ESA zur Erstellung verschiedener RTS und ITS (siehe Abbildung 4).

Artikel 37 „Folgemaßnahmen zuständiger Behörden“ stellt die „Gegenstelle“ zu den Artikeln 30 bis 36 dar und reiht sich im Zeitstrahl nach der Prüfung und den Empfehlungen der federführenden Aufsichtsinstanz ein. Und hier stellt Absatz 2 einen „Entscheidungswiderspruch“ dar, denn Finanzunternehmen müssen den Risiken Rechnung tragen, die in den Empfehlungen der federführenden Aufsichtsinstanz an kritische IKT-Drittanbieter ermittelt wurden. Diese Empfehlungen kennen die Finanzunternehmen mangels In-Kenntnissetzung durch die federführende Aufsichtsinstanz oder die zuständige Behörde nicht, sodass hier Asymmetrien zwischen Erwartungen der zuständigen Behörde und Finanzunternehmen an IKT-Drittanbieter entstehen können, die im unwahrscheinlichen Fall auch zu Feststellungen bei Aufsichtsobjekte führen könnten. Last but not least informiert Artikel 38 die IKT-Drittanbieter über die „Aufsichtsgebühren“, die diese für die Aufsicht durch ESA und die zuständigen Behörden zu entrichten haben.

Noch eine wichtige Randnotiz zu Fristen: Die beiden zentralen Artikel zu Prüfungen 23 und 24 gelten 3 Jahre nach dem Inkrafttreten von DORA, demnach aus heutiger Perspektive in fünf Jahren.

Handlungsempfehlungen für Finanzunternehmen und Aufsichten

Sowohl die Finanzunternehmen als auch die Aufsichten sollten nicht auf das Inkrafttreten der DORA warten. Auch wenn sich die final verabschiedete Fassung der DORA vom vorliegenden Entwurf unterscheiden wird, gehen die Autoren davon aus, dass sich wesentliche Inhalte nicht substanziell in Quantität oder Qualität ändern werden. Daher sollten beide Adressatengruppen mit der Vorbereitung auf die DORA beginnen, auch wenn diese vorerst in 2 Jahren in Krafttreten

möge. Eine Situation wie mit der DSGVO, die seit der Verabschiedung im Mai 2016 zwei Jahre später im Mai 2018 in Kraft und viele Marktteilnehmer „überrascht“ hat, sollte vermieden werden. Für ein Zuwarten stellt die DORA zu hohe Anforderungen an technisch-organisatorische Ausstattungen, an die Reife der Organisation im Risikomanagement und in der Informationssicherheit und an die Fähigkeiten der Verantwortlichen aller Beteiligten.

Zudem muss wohl unterschieden werden zwischen Finanzunternehmen, die solche Anforderungen wie aus der DORA bereits aus anderen Regulierungen kennen und Finanzunternehmen, für die die DORA der erste Anforderungskatalog zur Informationssicherheit darstellt. Zur ersten Gruppe gehören bspw. alle Banken, Versicherungsunternehmen und Zahlungsdienstleister, weil sie Anforderungswerke wie BAIT, VAIT und ZAIT erfüllen müssen. Zur zweiten Gruppe werden viele der neuen Adressaten der DORA gehören. Als Vorbereitungsschritte sind zu empfehlen:

1) Aufbau, Pilotierung und Betrieb eines zertifizierungsfähigen ISMS

Im regulierten Finanzsektor ist ein ISMS bereits Pflicht, jedoch ist die Bandbreite der Qualität der implementierten ISMS groß. Einer der Schwerpunkte des Managements sollte auf die Zertifizierungsfähigkeit der bisher Einsatz findenden ISMS gelenkt werden. Zudem besteht heute für viele der neuen Aufsichtsobjekte der DORA keine Pflicht zum Betrieb eines ISMS, sodass auf diese Finanzunternehmen erhebliche Aufwendungen zukommen. Sollte die Anforderung eines zertifizierten ISMS in der nächsten Regulierungsrunde eingeführt werden, stellt ein zertifizierungsfähiges ISMS die beste Vorbereitung dar.

2) Fokussierung auf Regelbereiche der DORA, Gap-Analyse und Mitigation von Feststellungen

Alle Finanzunternehmen sollten die Konformität ihrer Aufbau- und Ablauforganisation zu den vier Regelbereichen der DORA prüfen:

1. Anforderungen an IKT-Risikomanagement
2. Meldung von IKT-Vorfällen
3. Prüfung der digitalen Betriebsstabilität
4. Prüfung Risiko durch IKT-Drittanbieter

Mögliche Feststellungen durch Prüfer sollten präventiv beseitigt werden. Ein ISMS aus Schritt 1) stellt dabei eine solide sowie gleichfalls unabdingbare Basis für diesen zweiten Schritt dar.

3) Vorbereitung hybride IT-Prüfung

Finanzunternehmen und Aufsicht sollten gemeinsam einen Standard für eine hybride IT-Prüfung entwickeln. Die DORA wird weitere Digitalisierungsschritte einer Vielzahl von Prüfungshandlungen erzwingen. Ein hybrider Prüfungsansatz bestehend aus automatisch erfassten Größen (Maschinen basiert) und manuell durchgeführten Prüfungshandlungen (Experten basiert) bietet verschiedene Vorteile (siehe Abbildung 6) und reduziert Aufwände für Finanzunternehmen und Aufsicht.

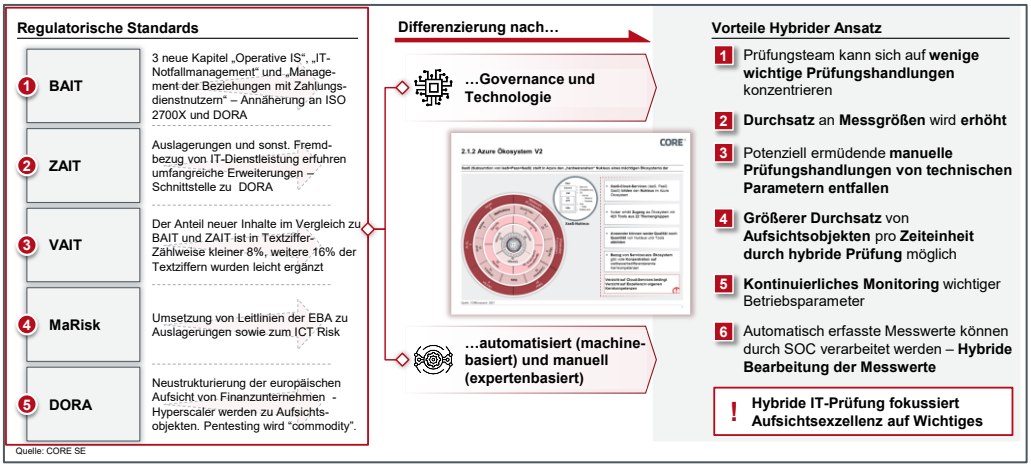


Abbildung 6: Zweifachhybride Perspektive auf Governance und Technologie

4) Aufsicht stärken

Die Aufsicht erfährt durch die DORA eine große Erweiterung ihrer Aufgaben in Quantität (Anzahl der Finanzunternehmen) und Qualität (vertiefte Kenntnisse in IKT und Risikomanagement), sodass eine angemessene Reaktion in Form von mehr Personal mit MINT-Kompetenzen notwendig wird. Die gemeinsame Entwicklung des hybriden IT-Prüfungsstandards mit Finanzunternehmen würde die Aufsicht verstärkt auf wesentliche Prüfungshandlungen und Aufsichtsinhalte fokussieren und ggf. zu einem europäischen Prüfungsrahmen beitragen.

Fazit

DORA wird zahlreiche bestehende Anforderungen an den Einsatz von modernen Technologien und dem Management von Risiken erstmals durch eine EU-weite Verordnung harmonisieren. Damit begründet DORA die erstmals EU-weit gültige Anwendung zahlreicher bestehender Anforderungen durch eine EU-Verordnung. Dieser Umstand begründet die Hoffnung auf eine deutliche Reduzierung der Aufsichts- und Prüfungsverwaltung für Finanzunternehmen, auf eine Beschleunigung der Digitalisierung im Finanzsektor und des weiteren Aufbaus an MINT-Kompetenzen, um Leitungs- als auch Aufsichtsgremien mit Know-how zu IKT-Organisation und Risikomanagement auszustatten.

Die Fähigkeit von Finanzunternehmen Cyberangriffen mit angemessenen Maßnahmen und Resilienz zu begegnen, drückt sich in den Themenschwerpunkten und dem Anforderungskatalog der DORA aus. Diese sind digitale Betriebsstabilität, Prüfung und der Einbezug von Risiken durch Outsourcing an IKT-Drittanbieter in das interne Risikoinventar von Finanzunternehmen. Die Aufsichtsobjekte tun gut daran, bereits jetzt die DORA zu antizipieren und ein Programm zur „Fitness DORA“ aufzusetzen – erste Schritte wären

1. Aufbau und Betrieb eines zertifizierungsfähigen ISMS,
2. Gap-Analyse der vier Themenschwerpunkte der DORA
    a. Anforderungen an IKT-Risikomanagement
    b. Meldung von IKT-Vorfällen
    c. Prüfung der digitalen Betriebsstabilität
    d. Prüfung Risiko durch IKT-Drittanbieter

und

3. die Vorbereitung einer hybriden IT-Prüfung.

Beide Adressatenkreise – Finanzunternehmen und die Aufsichtsorgane müssen ihre MINT-Fähigkeiten in Quantität und Qualität stärken.

Die europäische Harmonisierung des Aufsichts-, Prüfungs- und Sanktionswesens schafft eine vergleichbare und damit verlässliche und von allen Stakeholdern anerkannte, da vertrauenswürdige Basis. DORA bietet damit dem europäischen Finanzsektor enorme Chancen die Wettbewerbsfähigkeit zu verbessern und kann weiteren Sektoren als Vorbild im Thema Cyber-Sicherheit und Resilienz dienen.

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

Nadine Hofmann ist Senior Expert Managerin bei CORE. Sie studierte Luft- und Raumfahrttechnik in Braunschweig und Dresden. Ihre Beratungskompetenz fokussiert sich auf technischen Datenschutz und Informationssicherheit (insb. IAM, SOC/SIEM, Risikomanagement, ISO 27001 und DSGVO). Sie unterstützt Klienten bei der Strukturierung und dem Aufbau von Financial Compliance Systemen. Nadine fungiert als stellv. ISB.

Mail: nadine.hofmann@core.se

Holger Friedrich ist Managing Partner und einer der Gründer von CORE. Vor CORE gründete er Technologieunternehmen und war u.a. Partner einer führenden internationalen Strategieberatung. Er verfügt über langjährige Erfahrungen im Management umfassender IT-Transformationen und ist Experte im Technologiemanagement. Er unterstützt das Senior Management in Mission Critical Aufgaben, wie der der Durchsetzung regulatorischer Anforderungen.

Mail: holger.friedrich@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