Neue Anforderungen an IKT-Infrastrukturen im Finanzsektor

Marcus Scheidl

Gut zwei Jahre nach Veröffentlichung des Verordnungsentwurfs der Europäischen Kommission über die Betriebsstabilität digitaler Systeme des Finanzsektors, genannt „Digital Operational Resilience Act" oder kurz „DORA", zur Harmonisierung der Anforderungen in den EU-Mitgliedsstaaten sowie zur Steigerung der europäischen Cyber-Resilienz, haben das Europäische Parlament und der Europäische Rat der Verordnung nun im November 2022 zugestimmt. Bis zum Frühjahr 2023 soll das neue Regelwerk in Kraft treten.

Als Verordnung wird DORA in den Mitgliedstaaten unmittelbar gelten und ist somit von den in Artikel 2 (Geltungsbereich) gelisteten Finanzinstituten verbindlich anzuwenden. 24 Monate nach Inkrafttreten wird DORA dann verpflichtend – voraussichtlich Anfang 2025 – zur Anwendung kommen. Betroffene Finanzinstitute sind gut beraten, sich bereits jetzt einen Überblick über die kommenden Anforderungen an Informations- und Kommunikationstechnik (IKT)-Infrastrukturen zu verschaffen und ihren individuellen Handlungsbedarf zu bestimmen.

Die Einordnung von DORA in die bestehende Gesetzgebung und die aufsichtsrechtlichen Vorgaben

Die gesetzliche Grundlage ist in Deutschland das Kreditwesengesetz (KWG). Insbesondere über § 25a Abs. 1 KWG werden Mindestanforderungen an den ordnungsgemäßen Geschäftsbetrieb und das Risikomanagement und damit auch an die im Fokus von DORA stehende digitale Betriebsstabilität bzw. digitale operationale Resilienz von Finanzunternehmen adressiert.

Die betreffenden Anforderungen des KWG werden durch die Mindestanforderungen an das Risikomanagement (MaRisk) zuletzt mit ihrer 6. Novelle (Rundschreiben 10/ 2021 (BA)) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) konkretisiert. Die spezifischen nationalen bankaufsichtsrechtlichen Anforderungen an die Informations- und Kommunikationstechnik- Infrastrukturen (IKT) von Banken werden unter Bezugnahme und in Korrespondenz mit den MaRisk wiederum über die Bankaufsichtlichen Anforderungen an die Informationstechnologie (BAIT) in ihrer Novelle 2021 ausgeführt. In dieser kommen insbesondere auch die maßgeblichen Vorgaben aus den drei Leitlinien der europäischen Bankenaufsicht (EBA)

- für das IKT- und Sicherheitsrisikomanagement (EBA/GL/2019/04),
- zur Meldung schwerwiegender Sicherheitsvorfälle (im Rahmen der EU-Verordnung 015/2366 (PSD2)) sowie
- zu Auslagerungen (EBA/GL/2019/02)

zur nationalen aufsichtsrechtlichen Umsetzung.

Als Äquivalent zu den BAIT wurden für die Regulierung von Versicherungen durch die deutsche Aufsicht die Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) mit Rundschreiben 10/2018 in der Fassung vom 3. März 2022 und für die Beaufsichtigung der ebenfalls zum Geltungsbereich von DORA gehörenden Kapitalverwaltungsgesellschaften die Kapitalverwaltungsaufsichtlichen Anforderungen an die IT (KAIT) mit Rundschreiben 11/2019 (WA) veröffentlicht.

Darüber hinaus resultieren Anforderungen an die IKT- und Informationssicherheit bei deutschen Finanzinstituten aus dem IT-Sicherheitsgesetz (IT-SiG), dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, das in Deutschland zugleich den Grundstein der KRITIS-Regulierung darstellt. Das IT-SiG regelt seit 2015 mit dem BSI-Gesetz die Sicherheit Kritischer Infrastrukturen (KRITIS) und legt mit diesem Pflichten und Aufgaben von KRITIS-Betreibern und staatlichen Akteuren fest. Seit 2021 ist das IT-Sicherheitsgesetz 2.0 mit erweitertem Geltungsbereich (u.a. neue Sektoren) und ergänzten Pflichten für betroffene Unternehmen sowie erweiterten Rechten für das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Kraft. Die KRITIS-Verordnung 2021 brachte Erweiterungen bei den betroffenen KRITIS-Anlagen und Schwellenwerten u.a. bei Wertpapier- und Derivate-Transaktionen.

Zum besseren Verständnis der Zusammenhänge von EU-Verordnungen und nationaler Gesetzgebung mag der Hinweis genügen, dass mit dem IT-SiG die Umsetzung der europäischen NIS-Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit erfolgt. Das zuständige deutsche Bundesministerium des Innern und für Heimat (BMI) hatte die Anforderungen aus der NIS-Richtlinie bereits größtenteils vorwegnehmend im IT-SiG im Jahr 2015 berücksichtigt. Die NIS-Richtline wurde zuletzt zeitlich parallel zu DORA überarbeitet und wird zeitnah zu DORA als NIS2-Richtline in Kraft treten.

Wichtig zu wissen ist, dass DORA als sogenanntes „Lex Specialis" für den Finanzsektor als ausschließliche Anforderungsquelle im Bereich der digitalen betrieblichen IKT-Resilienz veröffentlicht wird und die relevanten Anforderungen aus NIS/NIS2 bereits inkludiert. Daher kann auch angenommen werden, dass über das deutsche IT-SiG zukünftig keine über DORA hinausgehenden Anforderungen an Finanzinstitute adressiert werden. Vielmehr ist ein expliziter Ausschluss von den durch DORA regulierten Finanzunternehmen aus dem Geltungsbereich des IT-SiG ein möglicher Schluss, wobei insbesondere die Schwellenwerte aus der BSI-KRITIS-Verordnung für den KRITIS-Betrieb ihre Gültigkeit behalten dürften.

Für die Praxis ist insgesamt von entscheidender Bedeutung, dass die aufsichtsrechtlich geforderten Vorfallmeldungen zukünftig sowohl an europäische als auch nationale Aufsichtsbehörden im Sinne einer möglichst effizienten Berichterstattung zu gleichen Meldeinhalten ohne Doppel- und Mehrfachaufwendungen erfolgen sollen.

Abb. 01: Wesentliche Regulierungsbereiche und -inhalte von DORA.

Quelle: Eigene Abbildung

DORA beinhaltet weitreichende Regelungen in fünf Regulierungsbereichen und delegierte Verordnungen für die Umsetzung durch die europäischen Aufsichtsbehörden

Wie ▶ Abb. 01 zeigt, kann DORA in fünf Regulierungsbereiche unterteilt werden, sofern man die Anforderungen an die Steuerung und Organisation, also die IKT-Governance, der angesprochenen Finanzunternehmen dem IKT-Risikomanagement (dann mit den Artikeln 5 bis 16) zuordnet. Artikel 17 bis 23 regeln die Meldung von IKT-bezogenen Vorfällen. Die Artikel 24 bis 27 bilden den Rahmen für die Überprüfung der digitalen Betriebsstabilität durch bedrohungsorientierte Penetrationstests (Threat-Led Penetration Testing, TLPT). Den aufsichtsrechtlich konformen Umgang mit IKT-Drittanbieter-Risiken klären die Artikel 28 bis 44. Der Informationsaustausch zur Cyberbedrohungslage und gewonnenen Erkenntnissen werden in Artikel 45 geregelt.

Grundlegendes Verständnis für die in DORA adressierten Anforderungen an die IKT von Finanzunternehmen und deren Umsetzung schafft der Artikel 4 mit dem Grundsatz der Verhältnismäßigkeit: „Die Finanzunternehmen wenden die in Kapitel II festgelegten Vorschriften im Einklang mit dem Grundsatz der Verhältnismäßigkeit an, wobei ihrer Größe und ihrem Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte Rechnung zu tragen ist." Diesem Grundsatz sollen gemäß DORA insbesondere auch die europäischen Aufsichtsbehörden (ESA) bei der ihren aufsichtsrechtlichen Umsetzungen folgen. Von grundlegender Bedeutung für diese sind die über DORA delegierten Verordnungen (Rechtsakte), mit denen die Erarbeitung entsprechender Leitlinien (Guidelines) bzw. technischer Regulierungs- bzw. Durchführungsstandards (Regulatory Technical Standards, RTS und Implementing Technical Standards, ITS) zur Umsetzung von DORA beauftragt werden. DORA verpflichtet die ESAs zur gemeinsamen Erarbeitung und Übermittlung gemeinsamer Entwürfe an die EU-Kommission nach 12, 18 oder in wenigen Ausnahmefällen 24 Monaten (je nach Regulierungsgegenstand) nach Inkrafttreten von DORA.

Ein Blick auf die Delegierten Verordnungen zeigt den nahenden Handlungsbedarf auf

Klar ist, dass DORA verschiedenste Neuerungen und Konkretisierungen bringt. Der Autor teilt einerseits die unverbindliche erste Einschätzung der deutschen Aufsicht BaFin, dass die Mehrzahl der Anforderungen zum IKT-Risikomanagement inkl. der geforderten Notfallvorsorge und zur Informationssicherheit bereits in den BAIT verankert und damit schon heute einen entsprechend hohen Erfüllungsgrad auf Seiten der beaufsichtigten Institute genießen.

Andererseits ist hinsichtlich des zu erwartenden Handlungsbedarfes der Finanzinstitute eine unterschiedlich stark ausfallende Ausdehnung bestehender Anforderungen speziell in den Regulierungsbereichen IKT-Vorfallmeldung, Testen der operationalen Resilienz (relevant zunächst für Finanzinstitute mit erhöhter Kritikalität für die die Finanzstabilität und/oder exponierten Risikoprofilen) und beim Management der Drittparteienrisiken aufgrund des neu einzuführenden europaweiten Beaufsichtigungsrahmens für IKT-Dienstleister erwartbar.

Tatsächlich kann eine Betrachtung der delegierten Verordnungen die Einschätzung zum Überprüfungs- und Handlungsbedarf erleichtern. Einige der an die ESAs gerichteten Beauftragungen für die aufsichtsrechtliche Umsetzung durch Leitlinien, RTS und ITS betreffen die kritischen IKT-Dienstleister. Dies ist zum Beispiel bei der Einstufung und Listenführung von kritischen IKT-Dienstleistern der Fall. Die meisten der delegierten Rechtsakte und die mit ihnen einhergehenden Umsetzungen der ESAs werden jedoch direkte Auswirkungen auf die Finanzunternehmen und damit die Banken haben.

Im Einzelnen sind in folgenden Regulierungsbereichen bzw. zu folgenden Artikeln entsprechende Konkretisierungen der ESAs mit direkter Relevanz für Finanzunternehmen beauftragt:

- **Artikel 11 (Reaktion und Wiederherstellung):** Leitlinien für die Schätzung der aggregierten jährlichen Kosten und Verluste

- **Artikel 15 (Weitere Harmonisierung von Tools, Methoden, Prozessen und Richtlinien für das IKT-Risikomanagement):** Festlegung weiterer Elemente für Richtlinien zu Verfahren, Protokollen und Tools für IKT-Sicherheit; Entwicklung weiterer Komponenten der Kontrollen von Zugangs- und Zugriffsrechten; Weiterentwicklung der Mechanismen zur umgehenden Erkennung anomaler Aktivitäten; Spezifizierung von genannten Komponenten der IKT-Geschäftsfortführungsleitlinie, Spezifizierung der Tests von IKT-Geschäftsfortführungsplänen; Spezifizierung der Komponenten der IKT-Reaktions- und Wiederherstellungspläne; Spezifizierung von Inhalt und Form des Berichts über die Überprüfung des IKT-Risikomanagementrahmens

- **Artikel 16 (Vereinfachter IKT-Risikomanagementrahmen):** Entwicklung von RTS für die Spezifizierung der Elemente des IKT-Risikomanagementrahmen sowie in Bezug auf Systeme, Protokolle und Tools zur Minimierung von Auswirkungen von IKT-Risiken und bzgl. der Komponenten der IKT-Geschäftsfortführungspläne als auch der Vorschriften über die Tests der Geschäftsfortführungspläne und Gewährleistung der Wirksamkeit der Kontrollen, nähere Spezifizierung von Inhalt und Form des Berichts über die Überprüfung des IKT-Risikomanagementrahmens

- **Artikel 18 (Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen):** Erarbeitung von RTS zur Präzisierung von Kriterien, einschließlich der Wesentlichkeitsschwellen für die Bestimmung schwerwiegender IKT-bezogener Vorfälle oder gegebenenfalls schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle, die der Meldepflicht unterliegen sowie von Kriterien zur Anwendung durch die zuständigen Behörden für die Bewertung schwerwiegender IKT-bezogener Vorfälle oder zahlungsbezogener Betriebs- oder Sicherheitsvorfälle

- **Artikel 20 (Harmonisierung von Inhalt und Vorlagen von Meldungen):** Erarbeitung von RTS zur Festlegung der Inhalte von Meldungen über schwerwiegende IKT-bezogene Vorfälle sowie erheblichen Cyberbedrohungen und deren Einordnung als solche; Festlegung von Fristen für Erst- und Folgemeldungen; gemeinsame Entwürfe technischer Durchführungsstandards zur Festlegung von Standardformularen

- **Artikel 26 (Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT):** Erarbeitung von RTS (im Einvernehmen mit der EZB im Einklang mit dem TIBER-EU-Rahmen) zur Präzisierung der Anforderungen und Standards für den Einsatz interner Tester, des Umfangs der TLPT, der Testmethodik und des Testkonzepts, der Ergebnisse, der Art der Zusammenarbeit bei der Umsetzung von TLPT und die länderübergreifende Anerkennung von Tests

- **Artikel 28 (Allgemeine Prinzipien (Management des IKT-Drittparteienrisikos):** Erarbeitung von ITS zur Festlegung der Standardvorlagen des Informationsregisters und Erarbeitung von RTS zur Spezifikation der Leitlinie-Inhalte in Bezug auf die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer und wichtiger Funktionen

- **Artikel 30 (Wesentliche Vertragsbestimmungen):** Erarbeitung von RTS zur Präzisierung von Aspekten der Risikobestimmung und -bewertung, bei der Weiterverlagerung von IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen

Überprüfungen des individuellen Status quo und des Handlungsbedarfs sind ab jetzt erforderlich

Alle fünf dargestellten Regulierungsbereiche von DORA adressieren neue und konkretisierende Anforderungen an Finanzinstitute in unterschiedlichem Ausmaß und Umfang. Schwerpunkte sind nicht zuletzt auch auf Basis der vorangestellten Betrachtung der delegierten Verordnungen beim IKT-Risikomanagement, insbesondere hinsichtlich der Anforderungen an Methoden und Prozesse, beim Meldewesen und der IKT-Dienstleistersteuerung sowie dem Testen der Cyber-Resilienz (wenn auch zunächst nur für ausgewählte Finanzinstitute) ersichtlich.

Die verbleibende Zeit von nunmehr zwei Jahren bis zur verpflichtenden Anwendung von DORA sollten Finanzinstitute aus Sicht des Autors und des Bundesverbandes Öffentlicher Banken Deutschlands (VÖB) in jedem Fall nutzen, um entlang der einzelnen DORA-Artikel und den enthaltenen Anforderungen ihren individuellen Status quo der Anforderungskonformität zu überprüfen, Handlungsbedarfe zu identifizieren und entsprechende Aktionspläne zu entwickeln. Aufgrund der aktuell noch in Gesamtheit fehlenden Kenntnis über die genauen aufsichtsrechtlichen Anforderungen der ESAs kann dabei ein detaillierter Abgleich der institutsindividuellen Konformität mit den einzelnen bestehenden aufsichtsrechtlichen Regelungen (u.a. den BAIT und den drei vorgenannten EBA-Leitlinien) ein guter Ausgangspunkt sein.

Literatur

Text-Quelle Artikel: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0381_DE.html#title2

Bild-Quelle Autorenfoto: VÖB

Autor

Marcus Scheidl

Direktor Zahlungsverkehr & Informationstechnologie, Bundesverband Öffentlicher Banken Deutschlands, VÖB, Berlin

Mitglied im Fachgremium IT der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

IMPRESSUM

Herausgeber:
Gesellschaft für Risikomanagement und Regulierung e.V.
Schwarzwaldstraße 42
D-60528 Frankfurt am Main
VR 14261 Amtsgericht Frankfurt am Main
info@ firm.fm, www.firm.fm

Verantwortlich für den Inhalt:
Frank Romeike,
RiskNET GmbH, Gesellschaft für Risikomanagement und Regulierung e.V.

Layout:
Uta Rometsch, Stuttgart

© Das Urheberrecht liegt bei den jeweiligen Autoren und Autorinnen sowie bei der Gesellschaft für Risikomanagement und Regulierung e.V., Frankfurt am Main 2023.
Die Artikel geben die Meinung der Autoren wieder und stellen nicht notwendigerweise den Standpunkt der Gesellschaft für Risikomanagement und Regulierung e.V. dar.
Vervielfältigung und Verbreitung, auch auszugsweise, mit Quellenangabe gestattet.

FIRM
Frankfurter Institut für
Risikomanagement und Regulierung

Gesellschaft für Risikomanagement und Regulierung e. V.
Schwarzwaldstraße 42
60528 Frankfurt am Main | Germany
Tel.: +49 (0) 69 87 40 20 00 | Fax: +49 (0) 69 87 40 20 09
info@firm.fm | www.firm.fm