RFC Professionals
SUSTAINABLE EXCELLENCE

plenum

Finanzsektor

Der Digital Operational Resilience Act (DORA)

so machen Sie sich fit!

Hintergrund, Timeline und Grundlagen von DORA

Der Digital Operational Resilience Act (DORA) wurde nach einem über zwei Jahre andauernden Konsultationsprozess mit Veröffentlichung im Amtsblatt der EU am 27.12.2022 finalisiert. Die Anforderungen treten zum 16.01.2023 in Kraft und sind spätestens nach 2 Jahren durch die betroffenen Unternehmen zu erfüllen.

Kernziel von DORA ist die Schaffung eines EU-weiten Rechtsrahmens mit einheitlichen Anforderungen zur Stärkung der EU-weiten Cybersicherheit und digitaler, operationeller Resilienz im Finanzsektor unter Einbezug der IT-Dienstleister. Hierdurch soll die Aufrechterhaltung der Funktionsfähigkeit und Wiederherstellungsfähigkeit des europäischen Finanzmarktes gewährleistet werden. Dazu wurde der Anwenderkreis gegenüber den bisherigen europäischen und nationalen Regularien deutlich erweitert.

Hintergrund sind zunehmende operationelle Risiken insbesondere in Verbindung mit der Informationssicherheit durch

- fortschreitende Digitalisierung u.a. im Zusammenhang mit der Corona Pandemie steigenden HomeOffice Anteils,
- politische Unsicherheiten und Bedrohungen durch Cyber- und Hackerangriffe sowie
- wachsende Nutzung von Dienstleistern (Cloud Diensten) und Einsatz von KI-Lösungen.

Timeline von DORA

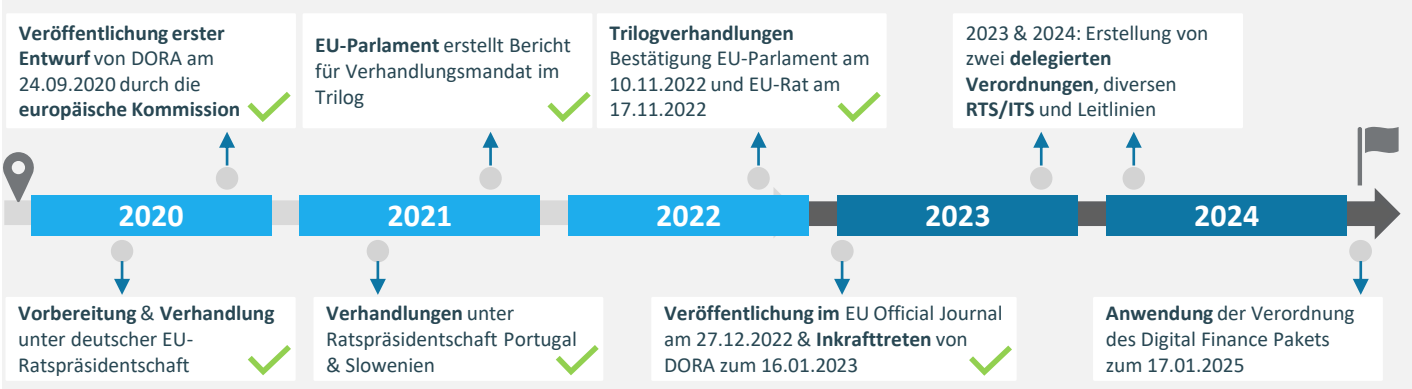


Abb. 1: Die DORA Zeitschiene

Struktur von DORA

Für die definierte breite Zielgruppe inkl. IKT-Drittdienstleistern sind die Anforderungen in Kapitel II bis V obligatorisch einzuhalten und damit operativ relevant. Kapitel VI regt den Informationsaustausch zwischen den betroffenen Unternehmen untereinander an.

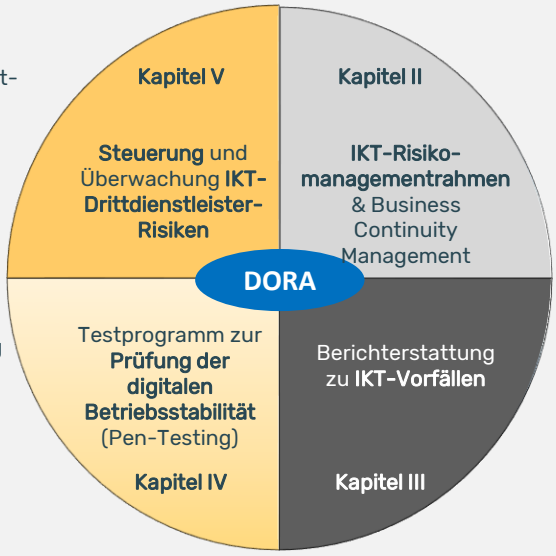
Die Regelungen aus den Kapiteln VII bis IX beinhalten formal-juristische Sachverhalte zur Umsetzung durch die Aufsichtsbehörden auf europäischer und nationaler Ebene.

I	Allgemeine Bestimmungen
II	IKT-Risikomanagement
III	IKT-bezogene Vorfälle
IV	Prüfung der digitalen Betriebsstabilität
V	Steuerung von IKT-Drittdienstleister-Risiken
VI	Vereinbarung über den Austausch von Informationen
VII	Zuständige Behörden
VIII	Delegierte Rechtsakte
IX	Übergangs- und Schlussbestimmungen

Abb. 2: Die Kapitelstruktur von DORA

Die Kernthemen von DORA im Überblick

- Register zu IKT-Drittdienstleistern
- Zusätzliche Anforderungen an die Überwachung des Risikos von IKT-Drittdienstleistern
- Weitreichende Untersuchungsrechte gegenüber IKT-Drittdienstleistern, abseits bestehender vertraglicher Rechte, für federführende Aufsichtsinstanz



- Erweiterte (operative) Pflichten des Managements bei der Steuerung des IKT-Risikomanagements
- Etablierung einheitlicher Vorgaben zu IKT-Störungen
- Vereinheitlichung des IKT-Risiko-managementrahmens
- Spezifizierung Anforderungen an BCM/ITSCM Notfallpläne

- Überprüfung kritischer IT-Systeme auf Betriebsstabilität und Absicherung in Bezug auf IKT-Störungen
- Penetrationstests inkl. Thread Led Penetration Tests (TLPT) für Produktionssysteme
- Formalisierter Prozess zum Testprogramm
- Beauftragung externer Tester

- Standardisierte Bearbeitung IKT-bezogener Vorfälle (Überwachung bis Reporting)
- Erweiterte Meldepflichten von schwerwiegenden IKT-Vorfällen

Abb. 3: Die Kernthemen von DORA

Überblick zu Neuerungen und Handlungsbedarfen

Zwar finden sich in DORA viele Vorgaben, die kongruent sind mit Vorschriften aus bestehenden Regularien, wie EBA-Leitlinien zu Auslagerungen und IKT sowie MaRisk/BAIT, MaGo/VAIT und KaMaRisk/KAIT. Allerdings enthält DORA auch einige Abweichungen, Detaillierungen und Ergänzungen gegenüber diesen Regularien. Der Anwenderkreis erstreckt sich grundsätzlich auf Kreditinstitute, Versicherungs- und Rückversicherungsunternehmen, Investmentfirmen, Zahlungsinstitute sowie IKT-Drittdienstleister.

Anpassungen mit zu erwartendem hohen Umsetzungsaufwand gegenüber bestehenden Regularien

Kap. II: IKT-Risikomanagementrahmen (Art. 5 - 16)

- Erweiterte Pflichten des Leitungsorgans bzgl. Genehmigungs-, Überwachungs- und Überprüfungshandlungen und damit verbunden eine regelmäßige Absolvierung von Fachschulungen zu IKT-Risiken
- Etablierung klarer Vorgaben zur Identifikation, Schutz & Prävention, Gegenmaßnahmen, Wiederherstellung und Kommunikation von IKT-Störungen
- Etablierung eines Prozesses für die Überprüfung und Auswertung von Erkenntnissen aus IKT-Vorfällen sowie Bereitstellung aktueller und vollständiger Informationen über IKT-Risiken an die zuständigen Behörden
- Verpflichtender Einsatz moderner IKT-Technologien und -Prozesse zum Schutz von Informationen sowie automatisierter Mechanismen zur Isolierung von betroffenen Informationsressourcen nach Cyberangriffen
- Vereinheitlichung des IKT-Risikomanagementrahmens hinsichtlich Vergleichbarkeit von Risiken mittels einheitlicher Metriken, Parameter und Risikoregister
- IKT-Pläne für die Wiederherstellung im Notfall sind einer unabhängigen Prüfung zu unterziehen. Erweiterung der Meldepflicht zu IKT-bezogenen Vorfällen um alle dadurch verursachten Kosten und Verlusten
- Bei IKT-Vorfällen & erheblichen Störungen der Haupttätigkeit sind Rückschauprüfungen zur Ermittlung von Verbesserungen, insbesondere hinsichtlich der Abläufe, inklusive Meldepflichten, obligatorisch

Kap. III: IKT-bezogene Vorfälle – Bewältigung, Klassifizierung & Berichterstattung (Art. 17 - 23)

- Standardisierte Überwachung (mit Frühwarnindikatoren) und Klassifizierung aller IKT-bezogenen Vorfälle
- Verpflichtende, detaillierte Aufzeichnung aller Tätigkeiten vor und während eines IKT-bezogenen Vorfalls
- Erheblich erweiterte Meldepflichten mit vorlagenbasierten Berichten zu schwerwiegenden IKT-Vorfällen an nationale Behörden sowie erweiterte Informationspflicht an Dienstnutzer und Kunden

Kap. IV: Prüfung der digitalen Betriebsstabilität (Art. 24 - 27)

- Testprogramm mit internen Validierungsmethoden die sicherstellen, dass sämtliche Sicherheitslücken schnellstmöglich geschlossen werden
- Vollständiges Spektrum geeigneter Tests inkl. konkreter Testverfahren wird vorgegeben
- Erweiterte Prüfungen von IKT-Instrumenten, -Systemen & -Prozessen auf Basis von Thread Led Penetration Tests (TLPT) im Turnus von 3 Jahren für kritische Funktionen & Dienstleistungen inkl. Auslagerungen
- Nachweispflicht der Qualifikationen interner und externer Prüfer/ Tester
- Testinhalte sind von der zuständigen Behörde zu genehmigen, und die Testergebnisse zum Erhalt einer Bescheinigung vorzulegen

Kap. V: Steuerung von IKT-Drittdienstleister-Risiken (Art. 28 - 44)

- Vorgabe eines Aufsichtsrahmens mit klarer Aufgabenzuweisung der führenden Aufsichtsinstanz und darin enthaltenen, weitreichenden Untersuchungsrechten auch gegenüber den IKT-Drittdienstleistern
- Führung eines Informationsregisters zu IKT-Drittdienstleistern (z.B. inklusive IT-Fremdbezüge)
- Durchführung einer Risikoanalyse und Vorhaltepflicht von Ausstiegsstrategien für die Inanspruchnahme von Leistungen der IKT-Drittdienstleister durch die Finanzdienstleister auch für IT-Fremdbezüge
- Finanzunternehmen müssen auch bei IT-Fremdbezügen bei der Vertragsgestaltung und der Überwachung des Risikos die Unterauftragsnehmer der IKT-Drittdienstleister, insbesondere aus Drittländern, berücksichtigen

Die erweiterten Anforderungen führen insgesamt zu einem umfangreichen Umsetzungsaufwand im Finanzsektor. Das individuelle Ausmaß ist dabei abhängig von der Größe (Proportionalitätsprinzip) und dem Reifegrad der digitalen operationalen Resilienz des jeweiligen Finanzdienstleisters.

Zeit zum Handeln - bestehende GAPs identifizieren

Die Vorgaben sind bis spätestens zum 17.01.2025 vollständig umzusetzen. Bei eventuellen Lücken ist die verbleibende Zeit zur Umsetzung ggf. eng bemessen. Inwiefern Ihr Haus konkreten Handlungsbedarf aufweist, können Sie in einem ersten Schritt mit unseren DORA delta self-assessment ermitteln: Falls Sie eine der Fragen nicht mit „Ja“ beantworten können, ist eine tiefergehende Analyse angeraten.

DORA delta self-assessment – Auszug aus dem Anforderungskatalog

Ausgewählte Fragestellungen von DORA	ja	tlw.	nein	?
II. IKT-Risikomanagementrahmen				
Beinhaltet der IKT-Risikomanagementrahmen Regelungen zu operativen Pflichten des Leitungsorgans bzgl. Genehmigungs-, Überwachungs- und Überprüfungshandlungen?	☐	☐	☐	☐
Wurden klare Vorgaben zur Identifikation, Schutz & Prävention, Gegenmaßnahmen, Wiederherstellung und Kommunikation von IKT-Störungen etabliert?	☐	☐	☐	☐
Besteht ein Prozess für die zeitnahe Überprüfung und Auswertung von Erkenntnissen aus IKT-Vorfällen sowie die Bereitstellung aktueller und vollständiger Informationen über IKT-Risiken (anhand vergleichbarer Werte)?	☐	☐	☐	☐
Werden moderne IKT-Technologien & -Prozesse zum Schutz von Informationen und zu einer Isolierung eingesetzt?	☐	☐	☐	☐
Werden IKT-Pläne für die Wiederherstellung im Notfall regelmäßig einer unabhängigen Prüfung unterzogen?	☐	☐	☐	☐
Sind Rückschauprüfungen bei IKT-Vorfällen und erheblichen Störungen vorgesehen?	☐	☐	☐	☐
III. IKT-bezogene Vorfälle				
Erfolgt eine standardisierte Überwachung und Klassifizierung aller IKT-bezogenen Vorfälle?	☐	☐	☐	☐
Werden alle Tätigkeiten vor und während eines IKT-bezogenen Vorfalls detailliert aufgezeichnet/ dokumentiert?	☐	☐	☐	☐
Liegen die für die vorlagenbasierten Berichte zu schwerwiegenden IKT-Vorfällen sowie Informationspflichten an Dienstnutzer und Kunden erforderlichen Daten vor?	☐	☐	☐	☐
IV. Prüfung der digitalen Betriebsstabilität				
Besteht ein vollumfänglichesTestprogramm mit geeigneten Tests, konkreten Testverfahren etc. und Validierungsmethoden?	☐	☐	☐	☐
Werden Thread Led Penetration Tests (TLTP) im vorgegebenen Turnus durchgeführt und sind die kritische Funktionen und Dienstleistungen, inkl. Auslagerungen, hierfür identifiziert?	☐	☐	☐	☐
Liegt ein Qualifikationsnachweis der internen und externen Tester vor?	☐	☐	☐	☐
Sind Mechanismen etabliert, welche die Genehmigung von Testinhalten durch die Aufsichtsbehörde und das Ergebnisreporting aufgreifen können?	☐	☐	☐	☐
V. Steuerung von IKT-Drittdienstleister-Risiken				
Beinhaltet das Informationsregister zu IKT-Drittdienstleistern bereits die IT-Fremdbezüge?	☐	☐	☐	☐
Bestehen Ausstiegsstrategien zu IKT-Drittdienstleistern und sind diese in den Verträgen verankert?	☐	☐	☐	☐
Werden auch bei IT-Fremdbezügen auch Unterauftragsnehmer der IKT-Drittdienstleister bei der Vertragsgestaltung und Überwachung des Risikos berücksichtigt?	☐	☐	☐	☐
Ist der Einbezug der Einstufung eines Dienstleisters als kritischer IKT-Drittdienstleister durch die Aufsicht im Rahmen der Risikoanalyse bereits vorgesehen oder sind diese einfach/schnell in bestehende Systematiken integrierbar?	☐	☐	☐	☐

Abb. 4: Ausgewählte Fragestellungen von DORA

Unser Fazit und Angebot - der DORA delta-check

Die Ergebnisse unseres Abgleichs von DORA mit bestehenden Regularien zeigen eine hohe Übereinstimmung der Anforderungen mit den in den DORA-Kapiteln enthaltenen Vorgaben. Trotzdem existieren einige wesentliche und viele punktuelle Elemente, welche die vorhandenen europäischen und nationalen Vorgaben konkretisieren oder verschärfen.

plenum und RFC Professionals führen seit vielen Jahren sehr erfolgreich regulatorische Projekte für die IT von Finanzunternehmen durch. Diese Erfahrung und Kenntnisse der Prüfungspraxis der Aufsicht kombinieren wir für Sie zu einem „DORA delta-check“, welcher Ihnen in kurzer Zeit Ihre individuellen Handlungsbedarfe aufzeigt. Als Partner der IT betrachten wir die IT und ihre Risiken hierbei „end-to-end“ entlang der Leistungsprozesse und gehen den Risikoursachen sorgfältig auf den Grund. Denn unser Auftrag endet nicht damit, die IT „durchzuprüfen”, sondern beginnt damit erst. Mit einem kompakten und ressourcenschonenden Vorgehen bieten wir Ihnen eine Standortbestimmung innerhalb weniger Wochen. Neben den Schwachstellen Ihrer IT aus Sicht der DORA Vorgaben zeigen wir Ihnen auf, mit welchen Sofortmaßnahmen Sie Ihre Compliance kurzfristig steigern können. Der wichtigste Mehrwert in unserem Vorgehen liegt jedoch darin, dass wir auf Basis unserer mehr als 25 Jahre Erfahrung mit Ihnen zukunftsorientierte Maßnahmen erarbeiten, die für eine angemessene & nachhaltige Compliance sorgen – damit Sie sich wieder voll auf Ihr Kerngeschäft konzentrieren können.

plenum AG
Management Consulting
THE SQUAIRE WEST 15 | Am Flughafen | D-60549 Frankfurt am Main
Telefon: +49 69 6435524-0 | Fax: +49 69 6435524-60 | Internet: www.plenum.de

RFC Professionals GmbH
Hauptstr. 112 | 65375 Oestrich-Winkel
Telefon: +49 6723 - 994 88 85 | Fax: +49 6723 - 994 95 28 |
Internet: www.rfc-professionals.com

Stand:
03.02.2023