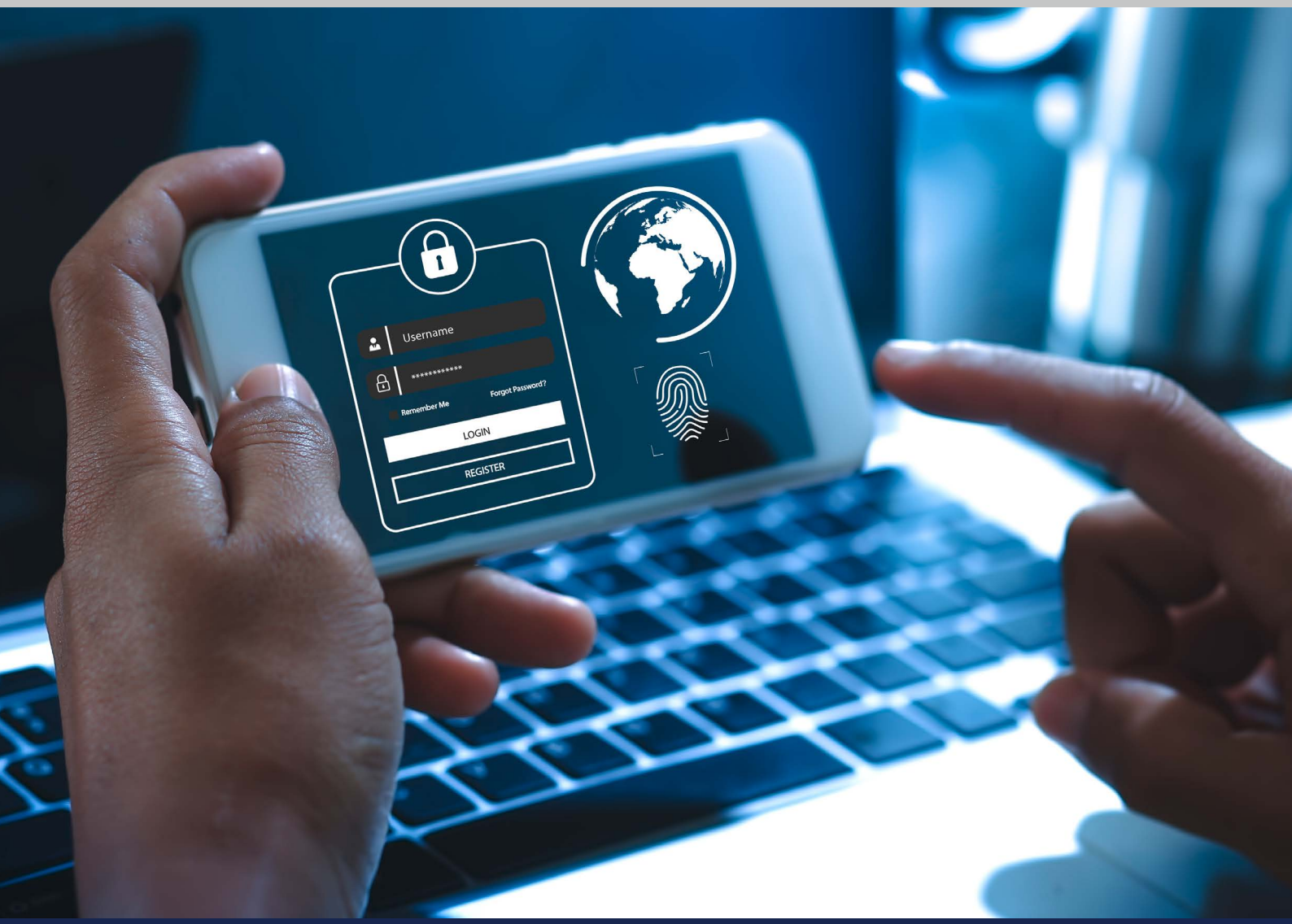
FORUM



DORA verstehen: Neue Anforderungen und Risiken für Finanzunternehmen

So setzen Sie die Digital Operational Resilience Act sicher und effizient um

Sehr geehrte Leser*innen,

DORA bringt neue, verbindliche Anforderungen an die digitale Resilienz von Finanzunternehmen. Insbesondere IT-Sicherheit, Risikomanagement und die Steuerung von Drittanbietern werden umfassend reguliert.

Für Unternehmen bedeutet das: bestehende Prozesse müssen überprüft, angepasst und dokumentiert werden. Gleichzeitig steigen die Anforderungen an Governance, Transparenz und Nachweisfähigkeit.

Dieses Whitepaper zeigt, welche konkreten Auswirkungen DORA hat und wie Finanzunternehmen die regulatorischen Vorgaben effizient umsetzen können – mit klaren Handlungsempfehlungen für die Praxis.

Über die Autorin:

Josefine Spengler ist Fachanwältin für IT-Recht und Expertin für Zahlungsdiensteaufsichtsrecht, IT- und Datenschutzrecht sowie Geldwäsche-Compliance. Sie berät insbesondere zu regulatorischen IT-Anforderungen im Finanzsektor und entwickelt praxisnahe Datenschutz- und Compliance-Konzepte. Als Spezialistin für das FinTech-Umfeld verbindet sie juristische Expertise mit technischem Verständnis und ist zudem Autorin des Blogs PAYMENT.TECHNOLOGY.LAW.

Alles über DORA – Auswirkungen und Handlungsempfehlungen für Finanzunternehmen

von **Josefine Spengler**, **Marina von Wallenberg-Pachaly**4. Juni 2024 7 Minuten

Was ist DORA?

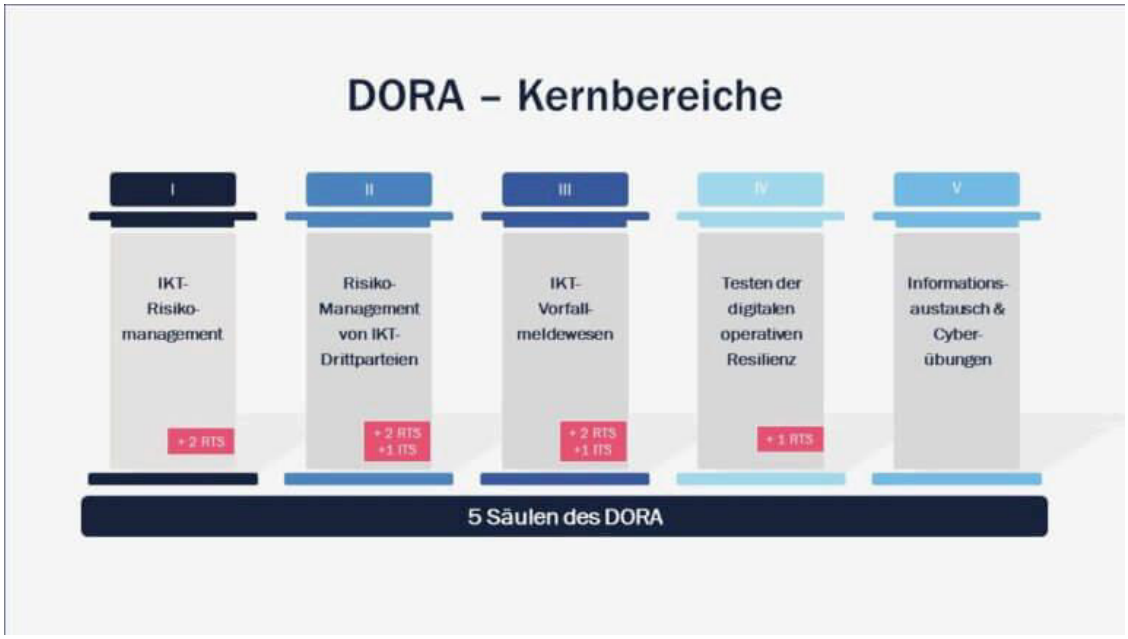
Mit DORA, der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act), verfolgt die Europäische Kommission das Ziel, einen einheitlichen Rahmen für ein effektives und umfassendes Management von Cybersicherheits- und IKT-Risiken in den Finanzmärkten zu schaffen.

Inhaltsverzeichnis

DORA ist „lex specialis“ zur NIS-2-Richtlinie, der Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (Network and Information Security Directive) und verschärft die Cybersicherheitsanforderungen in der gesamten EU für Banken und Finanzmarktinfrastrukturen. Aufgrund von DORA verlagert sich der Fokus der Finanzaufsicht weg von der Gewährleistung der finanziellen Widerstandsfähigkeit von Finanzunternehmen hin zur Sicherstellung der Aufrechterhaltung eines widerstandsfähigen IT-Betriebs im Falle einer schwerwiegenden Betriebsunterbrechung, die die Sicherheit des Netzes und der Informationssysteme gefährden könnte.

Parallel zu DORA werden auch Technische Regulierungs- (RTS) und Implementierungsstandards (ITS) veröffentlicht, die die Anforderungen des DORA weiter konkretisieren. Das erste Paket dieser RTS/ITS ist bereits zum 17.01.2024 veröffentlicht worden, das zweite Paket liegt im Entwurf vor und soll zum 17.07.2024 final veröffentlicht werden.

Inhaltlich lässt sich DORA in 5 Themenschwerpunkte aufteilen:



1. IKT-Risikomanagement

Mit DORA erhalten die Finanzunternehmen harmonisierte und EU-weit einheitliche Anforderungen an das IKT-Risikomanagement. Es werden neue bzw. verschärfte, aber auch erstmals konkrete Anforderungen an die IKT-Governance und Organisation, an den IKT-Risikomanagementrahmen, an IKT-Systeme, – Protokolle und -Anwendungen und an Weiterentwicklungen von IKT-Systemen sowie an Lernprozesse gestellt. Diese Anforderungen sollen dazu beitragen, die Funktionsfähigkeit der Finanzunternehmen insbesondere hinsichtlich Cyber-Gefahren aufrechtzuerhalten bzw. gegebenenfalls wiederherzustellen.

2. Management von IKT-Drittparteienrisiken

Von den Finanzunternehmen verlangt DORA eine Einschätzung und Überwachung der IKT-Drittparteirisiken – und zwar während des gesamten Lebenszyklus des Bezugs. Eine wichtige Voraussetzung hierfür ist, dass schon vor Vertragsabschluss eine Risikoanalyse und Due-Diligence stattfindet. Darüber hinaus legt DORA fest, welche Mindestanforderungen an die Vertragsinhalte mit IKT-Drittparteien gelten und dass alle IKT-Vertragsbeziehungen in einem Informationsregister (ähnlich dem Auslagerungsregister) eingetragen werden müssen. Das Informationsregister ist der Aufsicht auf Anforderung vorzulegen.

3. IKT-Vorfallmeldewesen

DORA enthält die Verpflichtung, einen Managementprozess zu implementieren, der neben der Behandlung von IKT-bezogenen Vorfällen auch die Überwachung, Protokollierung, Klassifizierung und ggfs. Meldung von IKT-bezogenen Vorfällen umfasst.

4. Testen der digitalen operationellen Resilienz

Finanzunternehmen müssen mit DORA ihre Informations- und Kommunikationstechnologie ständig überwachen und prüfen, indem sie ein risikobasiertes, proportionales Testprogramm etablieren sollen. Ein solches Testprogramm soll zum Beispiel Open-Source-Software analysieren, die Netzsicherheit und die physische Sicherheit in den Finanzunternehmen prüfen sowie Gap-Analysen, szenarienbasierte Tests, Kompatibilitätstests oder Penetrationstests umfassen. Auf diese Weise sollen die Finanzunternehmen unter anderem erkennen, wie sie auf IKT-Vorfälle vorbereitet sind und wo sie möglicherweise Schwachstellen in ihrer digitalen operationellen Resilienz haben.

5. Informationsaustausche und Cyberübungen

Zur Stärkung der digitalen operationellen Resilienz des europäischen Finanzsektors regt DORA an, dass Finanzunternehmen Informationen und Erkenntnisse über Cyberbedrohungen untereinander austauschen. Finanzunternehmen haben der zuständigen Aufsicht mitzuteilen, sobald ihr Mitwirken in solchen Information-Sharing-Vereinbarungen bestätigt wurde oder dieses endet.

Die BaFin und die Deutsche Bundesbank bereiten sich bereits jetzt auf DORA vor und arbeiten an der Anpassung ihrer Aufsichts- und Verwaltungspraxis und der Implementierung von IT-Prozessen und -Systemen im Rahmen von DORA. Zukünftig wird die BaFin zum nationalen Melde-Hub für IKT-Vorfälle im Finanzsektor. Des Weiteren nimmt die BaFin Anzeigen im Rahmen des IKT-Drittparteimanagements entgegen, zu denen die Institute und Unternehmen verpflichtet sind, und analysiert sie mit Blick auf potenzielle Risiken für den Finanzsektor.

Ab wann gilt DORA?

- **Inkrafttreten:** seit 16.01.2023
- **Umsetzungsfrist**: 2 Jahre, also bis zum **17.01.2025**

DORA gilt ab dem 17.01.2025 unmittelbar und betrifft alle beaufsichtigten Institute und Unternehmen des europäischen Finanzsektors sowie ihre IT-Auslagerungsdienstleister

Für wen gilt DORA?

DORA gilt – mit wenigen Ausnahmen – grundsätzlich für alle regulierten Finanzunternehmen in der EU und insbesondere auch für IKT-Drittdienstleister.

Im Vergleich zu den beiden EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken und EBA-Leitlinien zu Outsourcing bezieht DORA eine größere Anzahl und weitere Arten von Finanzunternehmen in den Anwendungsbereich ein (vgl. Art. 2 (1) DORA), u.A.:

- Kreditinstitute,
- Zahlungsinstitute,
- Versicherungen
- Wertpapierfirmen,
- Handelsplätze,
- Anbieter von Kryptodienstleistungen,
- Ratingagenturen,
- Schwarmfinanzierungsdienstleister,
- IKT-Dienstleister (Die Definition in Art. 3 Nr. 21 DORA erfasst u.a. Anbieter von Cloud-Computing-Diensten, Software, PSPs Datenanalysedienste und Rechenzentren für Finanzunternehmen sowie Anbieter von Kernbankensystemen.)

Welche Auswirkungen hat DORA für Finanzunternehmen?

Trotz der Umsetzungsfrist bis zum 17.01.2025 existiert bereits jetzt starker Druck bei Finanzunternehmen, den Handlungsbedarf aus den DORA-Anforderungen zu identifizieren und umzusetzen. Da keine Übergangsfrist gilt, müssen die Anforderungen zum Stichtag 17.01.2025 umgesetzt sein. Der Fokus wird auf der Einführung eines **umfassenden IKT-Risikomanagements**, einschließlich verschiedener IKT-Strategien, -Verfahren und -Werkzeuge zur Identifizierung von Risiken, zum Schutz von IKT-Systemen und zur Minderung des Risikos von Cybersicherheitsvorfällen, zur Erkennung anomaler Aktivitäten, zur Wiederherstellung

nach widrigen Ereignissen und zum Einsatz von Backup- und anderen Wiederherstellungsmethoden, liegen.

Mit DORA wird erneut herausgestellt, dass die Gesamtverantwortung für das IKT-Risikomanagement bei der Geschäftsleitung verortet ist, da nur die Geschäftsleitung den unternehmerischen Gesamtüberblick hat und entsprechend sinnvolle Entscheidungen treffen kann. Aufgrund der ständig wechselnden Cyberbedrohungslage müssen Finanzunternehmen nach den Vorgaben des DORA ihre IKT-Systeme durch regelmäßige Updates stabilisieren, Schwachstellen proaktiv managen und präventive Maßnahmen ergreifen. Im Schadensfall sind ausgereifte Business Continuity- und Wiederherstellungsstrategien sowie regelmäßige Schulungen der Mitarbeiter erforderlich.
Ein zweiter Schwerpunkt von DORA ist die Anforderung, dass die eigene **betriebliche Widerstandsfähigkeit regelmäßig getestet** wird. Die Tests sollten eher risikobasiert als standardisiert durchgeführt werden – von den Finanzinstituten wird erwartet, dass sie die Risiken testen, die für ihre Wertpapierdienstleistungen und Geschäftsbereiche am wichtigsten sind. Damit soll sichergestellt werden, dass die Cyber-Risikokontrollen der Unternehmen auf ihr jeweiliges Geschäft zugeschnitten sind.
Darüber hinaus müssen Finanzunternehmen (ähnlich der Meldung nach § 54 ZAG) die Analyse, Klassifizierung und Dokumentation **von IKT-bezogenen Vorfällen und deren Meldung** an die zuständige Aufsichtsbehörde sicherstellen.

DORA verlangt auch, die **Risiken im Zusammenhang mit Dienstleistungen Dritter zu bewerten** und Richtlinien zu haben, die sicherstellen, dass nur geeignete Dienstleistungen Dritter in Anspruch genommen werden. Da der Finanzsektor vermehrt auf große Technologieanbieter für ihre IKT-Infrastruktur und Cloud-Services setzt, wobei hauptsächlich die global größten Firmen genutzt werden, treten immer stärkere IKT-Konzentrationsrisiken auf, die von Finanzunternehmen frühzeitig erkannt und adressiert werden müssen.

DORA legt außerdem fest, welche **Mindestvertragsklauseln** Auslagerungsverträge enthalten müssen, wobei zwischen nicht-kritischen und kritischen (wesentlichen) IKT-Dienstleistungen unterschieden wird.

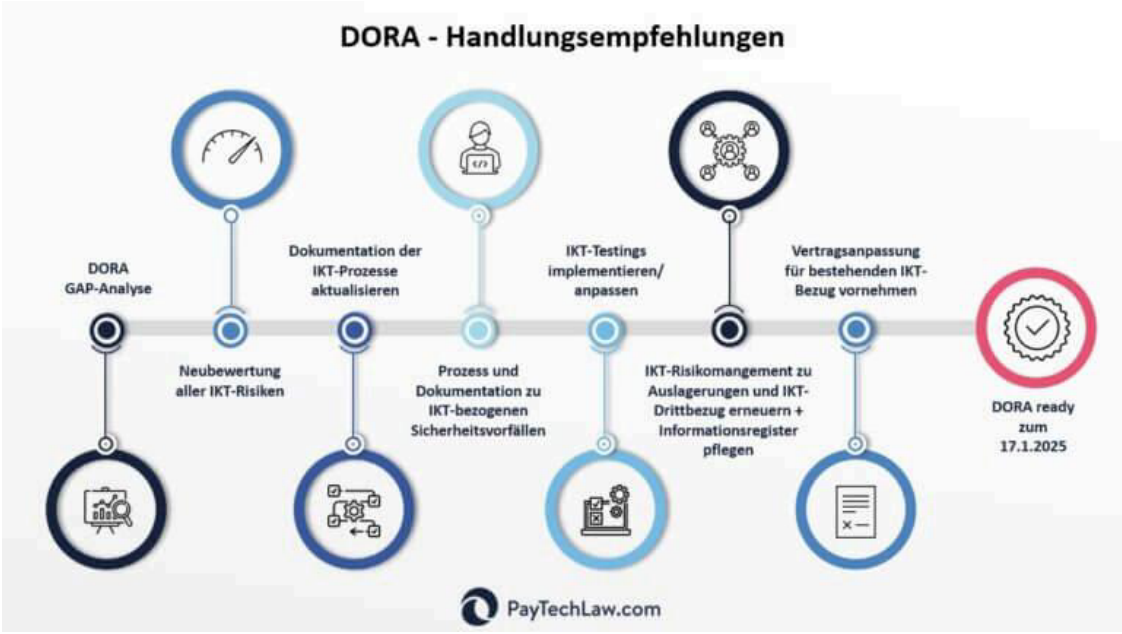
Im Rahmen des Risikomanagements sind Finanzunternehmen gemäß Art. 28 Abs. 3 DORA verpflichtet, ein **Register aller ausgelagerten IKT-Dienstleistungen** zu führen. Für dieses Register existieren mit DORA spezifische Anforderungen an Format und Inhalt, die in einem eigenen Technischen Implementierungsstandard festgelegt wurden. Zudem sind bei Auslagerungen, besonders in Drittländer, sorgfältige Due-Diligence-Prüfungen erforderlich.
Mit DORA ist die interne Organisationsstruktur durch **Einrichtung neuer Funktionen** anzupassen. Während es bisher im Rahmen des internen Kontrollsystems

eine Risikocontrolling-Funktion, eine Compliance- Funktion sowie einen Informationssicherheitsbeauftragten gibt, ist gemäß DORA eine neue unabhängige Kontrollfunktion für das Management und die Überwachung des spezifischen IKT-Risikos einzurichten. Die „IKT-Risikomanagement-Funktion“ muss von anderen Kontrollfunktionen und der Innenrevision getrennt sein.

Zudem ist gemäß Art. 5 Abs. 3 DORA eine Funktion zur Überwachung von Verträgen über die Nutzung von IT-Dienstleistungen einzurichten oder ein Mitglied der Geschäftsleitung dafür zu benennen. Diese Funktion dürfte mit dem Auslagerungsbeauftragten, den die BAIT/ZAIT bereits vorgeben, kongruent gehen.

Des Weiteren ist eine Krisenmanagementfunktion einzurichten, die bei der Aktivierung von IKT-Geschäftsfortführungsplänen bzw. Reaktions-/Wiederherstellungsplänen u.A. für die Festlegung von Verfahren für die Abwicklung interner und externer Krisenkommunikation verantwortlich ist.

Handlungsempfehlungen



Mit Blick auf die sich nähernde Umsetzungsfrist bis zum 17.01.2025 sollten Finanzunternehmen mit der Bewertung der Implikationen von DORA und der Umsetzung der DORA-Anforderungen sofort beginnen. DORA konkretisiert die bereits bestehenden Regulierungen und Standards zu den Anforderungen an die IT von Finanzunternehmen und erweitert sie in einem Umfang, der je nach Art des Finanzunternehmens und dem bisher erreichten Reifegrad der Umsetzung der aktuellen regulatorischen Anforderungen an die IT einen erheblichen Umsetzungsbedarf auslöst. Finanzunternehmen sind daher angehalten, die DORA-Anforderungen bereits jetzt zu

prüfen, entsprechende **GAP-Analysen** in ihrem Unternehmen durchzuführen und die umfangreichen Änderungen umzusetzen.

Alle **IKT-Risiken müssen neu evaluiert** und in das gesamte Risikomanagementsystem von Instituten integriert werden. Dabei ist die Definition einer nachvollziehbaren, überschneidungsfreien und an die Risikoverteilung eines Instituts angepassten Risikotaxonomie/-methodik erfolgskritisch, damit z.B. die Zuordnung, Steuerung und Verantwortung für Informations- und Outsourcing-Risiken oder Cyber-Risiken klar definiert sind.
Durch die bereits (teils noch im Entwurf) vorliegenden technischen Regulierungs- und Durchführungsstandards zu DORA (DORA-RTS/DORA-ITS) ist bereits klar, dass gerade im Bereich des IKT-Risikomanagements ein erheblicher Mehraufwand zur **Dokumentation der IKT-Prozesse und IKT-Systeme** erforderlich ist. So sieht der DORA-RTS zum IKT-Risikomanagementrahmen (Art. 15 DORA) mehr als 20 verschiedene interne IKT-bezogene Richtlinien (u.A. zum IKT Asset Management, zu Verschlüsselung und kryptografische Kontrollen, zum Kapazitäts- und Leistungsmanagement, zur Daten- und Systemsicherheit, zum Logging, zur Netzwerksicherheit, zum Change Management, zum Access Monitoring, zum Monitoring der IKT-Systeme, zum Management von IKT-bezogenen Sicherheitsvorfällen, zur IKT-bezogen Geschäftsfortführung im Krisenfall und zum Testen diverser Notfallpläne, aber auch zum Testen der IKT-Systeme) vor.

Darüber hinaus müssen Finanzunternehmen gemäß Art. 17ff. DORA einen Prozess für die **Behandlung IKT-bezogener Vorfälle** entwickeln, um diese und erhebliche Cyberbedrohungen zu erkennen und zu mitigieren. Schwerwiegende IKT-bezogene Vorfälle (dies sind IKT-Vorfälle, die umfassende nachteilige Auswirkungen auf die Netzwerk- und Informationssysteme haben, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen) müssen an die BaFin und gegebenenfalls auch an Betroffene gemeldet werden.

DORA fokussiert verstärkt auf der Prävention von IT- und Cyberbedrohungen und gibt daher konkrete Vorgaben für das Testen der digitalen operationalen Resilienz, die als integraler Bestandteil des IKT-Risikomanagements umgesetzt werden müssen. Hierzu sind **Anpassungen oder Neu-Implementierungen von Testing-Prozessen** und den entsprechend dazugehörigen Dokumentationen erforderlich. Die BAIT/ZAIT sehen zwar bereits eine regelmäßige bzw. anlassbezogene Überprüfung der Sicherheit der IT-Systeme, z.B. durch Penetrationstests, vor, aber durch DORA werden die Anforderungen an solche Tests präzisiert und durch die dezidierte Forderung von bedrohungsorientierten Tests (Threat-Led-Penetration-Tests, TLPT) verschärft.

Zwar gibt es einige Überschneidungen der DORA mit den Vorschriften der EBA-Leitlinien für die Auslagerung, aber die Vorschriften sind nicht vollständig kohärent

und DORA führt einige neue Mindestanforderungen an Auslagerungsverträge ein. Aufgrund dieser Divergenz können Finanzunternehmen nicht davon ausgehen, dass eine Auslagerungsvereinbarung, die mit den EBA-Vorschriften übereinstimmt, automatisch auch die Einhaltung von DORA gewährleistet. Die Unternehmen sollten ihre **aktuell bestehenden Verträge mit IKT-Dienstleistern** daher mit den Anforderungen von DORA vergleichen und Maßnahmen ergreifen, um sicherzustellen, dass alle festgestellten Lücken vor Ablauf des Umsetzungszeitraums geschlossen werden. DORA kennt keine Ausnahme für bereits bestehende IKT-Verträge, so dass diese angepasst werden müssen. Um bei der Anpassung von IT-Dienstleistungsverträgen alle Mindestinhalte nach DORA rechtssicher zu berücksichtigen, sind fachliches/technisches Verständnis der an Dritte vergebenen Dienstleistung, Erfahrung mit bestehenden EBA/BaFin-Regelungen und juristisches Know-how erforderlich. Bei laufenden Regulierungsinitiativen sollten bereits die neuen Anforderungen in den DORA-relevanten Bereichen berücksichtigen, um Synergien zu schaffen. Da DORA nicht zwischen Auslagerungen und sonstigem Fremdbezug von IKT-Dienstleistungen unterscheidet (sondern zwischen nicht-kritischen und kritischen/wesentlichen IKT-Funktionen), müssen die Mindestanforderungen an IKT-Verträge aus der DORA ggfs. auch Vertragsbeziehungen, die im aktuellen Auslagerungsregister nicht enthalten sind. Das neue **IKT-Informationsregister** ist (ähnlich und parallel zum Auslagerungsregister) mit all seinen Anforderungen an Inhalt und Format einzuführen und ab dem 17.01.2025 stets aktuell zu halten.

TAGS: Bafin DORA Risikomanagement

Praxiswissen für Ihren Erfolg im Job

Seminare zu Kredit und Finanzierung

Erfahren Sie in unseren Weiterbildungen praktisches und aktuelles Know-how zu unterschiedlichen Themen der Kredit- und Bonitätsanalyse sowie Kreditvergabe und Finanzierung. Jetzt informieren.

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.
Jetzt testen.

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

FORUM · Institut für Management GmbH • Postfach 10 50 60 • 69040 Heidelberg • Germany
Telefon: +49 6221 500-500 • Fax: +49 6221 500-555 • www.forum-institut.de