

Digital Operational Resilience Act

Neuerungen und Herausforderungen

28.09.2022

Digital Operational Resilience Act (DORA) stellt neue Anforderungen an Finanzinstitute und IT-Dienstleister

Im September 2020 wurde DORA, ein Vorschlag für eine neue Verordnung des Europäischen Parlaments und des Rates, veröffentlicht.







DORA stellt neue Anforderungen an das Informationssicherheitsmanagement von regulierten Finanzinstituten und bisher nur indirekt betroffenen IKT-Dienstleistern.

Betroffene Institute und Unternehmen müssen sich auf die voraussichtlich in diesem Jahr relevant werdende Verordnung vorbereiten.



Relevante Stakeholder des Digital Operational Resilience Act

Finanzunternehmen

-  Kreditinstitute
-  Zahlungsinstitute
-  Wertpapierfirmen
-  Anbieter von Krypto-Dienstleistungen
-  (Rück-)Versicherungsunternehmen
-  und 15 weitere Unternehmenstypen

Europäischen Aufsichtsbehörden

- **EBA:** Europäische Bankenaufsichtsbehörde
- **ESMA:** Europäische Wertpapier- und Marktaufsichtsbehörde
- **EIOPA:** Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung
- **Gemeinsamer Ausschuss:** Gremium der ESA, ESMA und EIOPA mit Vertretern der EZB, der ENISA und weiteren Beobachtern.

+

Kritische IKT-Drittanbieter nach einer Definition des Gemeinsamen Ausschusses

DORA: Schwerpunkte und Ziele

Governance



Aktive Rolle des Leitungsorgans bei der Steuerung des IKT-Risikomanagement.



Zuweisung von angemessenen Haushaltsmitteln.



Verpflichtende Fachschulungen für die Mitglieder des Leitungsorgans.

Systemischer Blick



Berücksichtigung von Risiken gegenüber und durch andere Finanzunternehmen.



Ermittlung der Vernetzung von IKT-Drittanbietern.

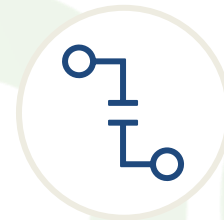


Berücksichtigung der potentielle Gesamtauswirkungen auf Markteffizienz bei den Wiederherstellungszeiten.

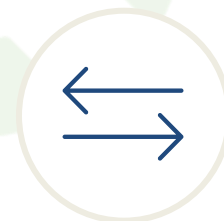
Förderung der Resilienz



Transparenzanforderungen an und Prüfung von BCM auch außerhalb von KRITIS.



Umsetzung automatisierter Mechanismen zur Isolierung von Informationsressourcen und Netzsegmenten.



Optionen zum Informationsaustausch zu Bedrohungen.

IKT-Drittanbieter



Trends im Finanzmarkt im Hinblick auf IKT-Drittanbieter



Weiter beständiger Trend zur Auslagerung von IKT-Services.



Leistungstiefen der genutzten ITK-Services werden höher, damit steigt die Verantwortung für Informationssicherheit bei den ITK-Drittanbietern.



Durch hochgradige Spezialisierung von Anbietern entstehen teils fragmentierte Wertschöpfungsketten und verschachtelte Lieferketten.



Teilweise gibt es eine direkte Konzentration auf einige wenige Anbieter im Markt, teilweise entstehen indirekte Konzentrationsrisiken durch Bündelung von Weiterverlagerungen bei einigen wenigen Anbietern.

Gesetzgeber sieht eine unzureichende Steuerung externer Quellen von IKT-Risiken im Finanzmarkt und schafft hierfür mit DORA einen einheitlichen Rahmen.

Herausforderungen bei Steuerung externer Quellen für IKT-Risiken



Komplexe vertragliche Gestaltungen, speziell bei sehr großen Anbietern (bspw. Cloud Service Provider).



Beschränkte Möglichkeiten zur Umsetzung individueller Vertragsgestaltungen für das einzelne Finanzinstitut.



Hochgradig standardisierte Services die ggf. nicht den speziellen Anforderungen des Finanzinstituts entsprechen.



Nicht ausreichende Transparenz und damit unvollständiges Monitoring der gesamten Service Lieferkette inklusive der Subdienstleister.



Marktmacht großer Anbieter im Verhältnis zu einem Finanzinstitut.

Speziell von Bedeutung bei Auslagerung von kritischen Funktionen an IKT-Drittanbieter.

Zukünftig direkte Beaufsichtigung kritischer IKT-Drittanbieter durch die Aufsichtsbehörden.

Risiko durch IKT-Drittanbieter

Transparenz und Berichterstattung



Jährliche Berichtspflicht an Behörde über neue - und auf Anfrage Gesamtübersicht der genutzten - IKT-Drittanbieter in Form eines Registers.



Zeitnahe Unterrichtung der Behörde über geplante Auslagerungen von kritischen oder wichtigen Funktionen.



Hierzu werden von den ESA noch technische Durchführungsstandards bzw. Regulierungsstandards erarbeitet.

IKT-Konzentrationsrisiko

Spezifische Berücksichtigung des IKT-Konzentrationsrisikos durch nicht ersetzbare oder mehrfache Vereinbarungen mit stark verbundenen IKT-Drittanbietern inkl. Berücksichtigung der Unterauftragsvergabe an weitere IKT-Drittanbieter.

Technische Regulierungsstandards (RTS):
u.a. detaillierter Inhalt der erforderlichen Policy für die Nutzung von IKT-Diensten, die von IKT-Drittanbietern erbracht werden, unter Bezugnahme auf Hauptphasen des Lebenszyklus der jeweiligen Vereinbarungen

Deep Dive: Kriterien für kritische IKT-Drittanbieter

Kriterien für kritische IKT-Drittanbieter

- Systemische Auswirkungen auf Stabilität, Kontinuität oder Qualität
- Systemische Bedeutung der Finanzunternehmen, die den Drittanbieter nutzen
- Direkte oder indirekte Abhängigkeit der Finanzunternehmen von IKT-Drittanbietern, die ein Konzentrationsrisiko darstellen
- Substituierbarkeit des IKT-Drittanbieters
- Zahl der Mitgliedsstaaten, in denen der IKT-Drittanbieter Dienstleistungen erbringt
- Zahl der Mitgliedsstaaten, in denen die Finanzunternehmen tätig sind, die einen IKT-Drittanbieter nutzen

Umgang mit kritischen IKT-Drittanbietern



ESA **veröffentlichen** jährlich und aktualisieren jährlich die **Liste kritischer IKT-Drittanbieter**.



Freiwillige Aufnahme eines IKT-Drittanbieters in die Liste ist auf **Antrag** an eine ESA möglich.



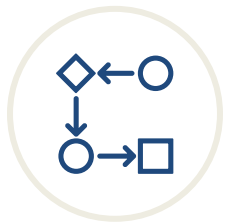
Finanzunternehmen dürfen **keinen IKT-Drittanbieter mit Sitz in einem Drittland** in Anspruch nehmen, welcher nach den Kriterien als kritisch eingestuft würde, wenn er seinen Sitz in EU hätte.

Prüfung der digitalen Betriebsstabilität



Prüfung der digitalen Betriebsstabilität

Die Institute sollen ein Programm zum Testen der digitalen Betriebsstabilität etablieren um auf IKT-relevante Vorfälle vorbereitet zu sein und allgemeine Schwächen zu identifizieren bzw. zu vermeiden.



Die Institute müssen Prozesse etablieren, um die Erkenntnisse der Tests zu priorisieren, klassifizieren und beheben und verifizieren, dass die identifizierten Schwächen behoben wurden.



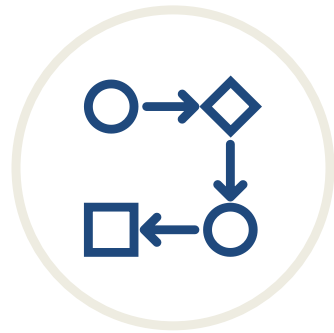
Prüfung von IKT-Tools und Systemen, z. B. durch Penetrationstests, Schwachstellenscans, Gap-Analysen oder Überprüfungen der physischen Sicherheit.



Durchführung von bedrohungsbasierten Penetrationstests.

Tests dürfen durch unabhängige interne und externe Parteien durchgeführt werden.

Deep Dive: Bedrohungsorientierte Penetrationstests



Kritische Prozesse erheben



Bedrohungen identifizieren



Penetrationstest durchführen



Behebung planen



Aufsicht informieren

Konkretisierung



Betroffene Finanzunternehmen werden durch die Aufsichtsbehörden auf Basis der **Größe**, dem **Umfang der Geschäftsaktivitäten** und dem **Risikoprofil** ausgewählt.



Durch einen RTS werden das Vorgehen für das **Festlegen des Umfangs**, das **Vorgehensmodell** für bedrohungsorientierte Penetrationstests und der **Umgang mit den Testergebnissen** festgelegt.

Ausblick

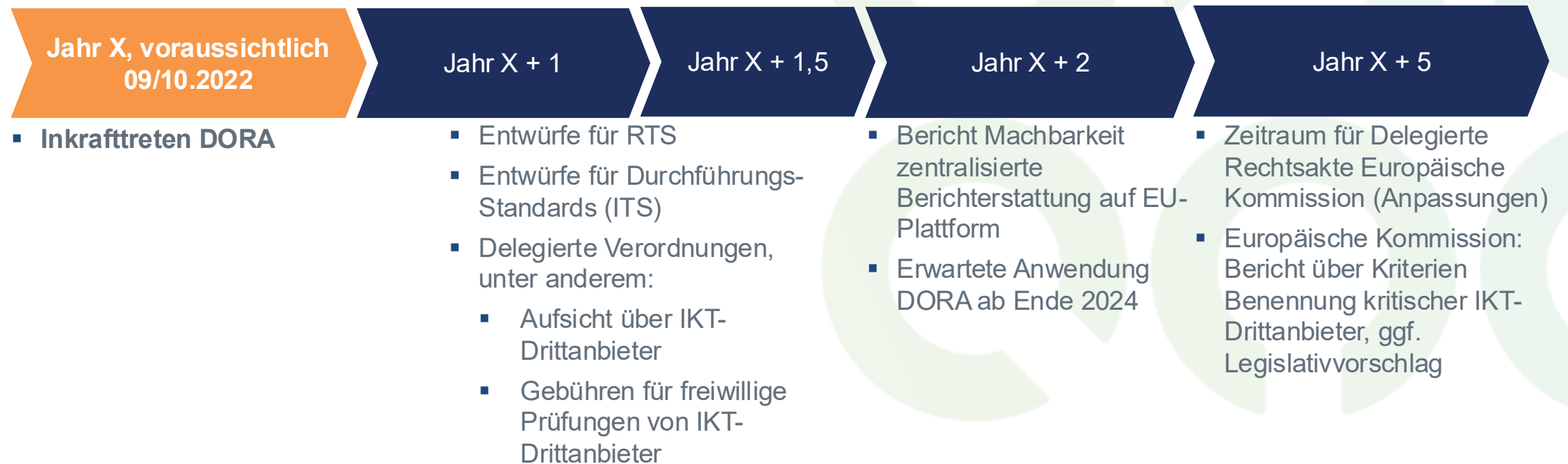


Zeithorizont

Die EU-Kommission, der europäische Rat und das EU-Parlament haben eine endgültige Fassung des Digital Operational Resilience Acts beschlossen.

Folgende Meilensteine sind bereits vorgesehen und terminiert.

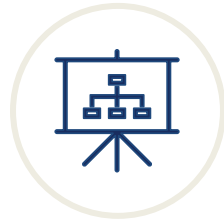
Timeline



Inkrafttreten DORA

20 Tage nach Veröffentlichung im Amtsblatt der Europäischen Union

Der Gesetzgeber erwartet (mit gewissen Erleichterungen für Kleine und Kleinstunternehmen)



Interne Governance

- Geschäftsstrategie
- IT- und IT-Sicherheitsstrategie
- Risikostrategie



Umfassende Prozess-, System- bzw. Tool-Landkarten mit zugewiesener (Risiko-) Verantwortlichkeit



Einrichtung von zwei Stellen:

- Risikomanagement-Funktion
- Krisenkommunikations-Funktion



Handlungsprotokolle z.B. von

- IKT-bezogenen Vorfällen
- Unterbrechungen des Geschäftsbetriebs ausgeführten Wiederanlaufplänen
- durchgeführten Pen-Tests



... auf deren Basis sich Risiken sowohl ablauftechnisch als auch finanziell bemessen lassen



.. sodass die Aufsicht Existenz, fortlaufende Überprüfung, Angemessenheit und Wirksamkeit bewerten kann



DORA ist Lex Specialis für NIS(2) als auch PSD2 und verweist ausdrücklich auf die DSGVO

RTS und ITS Veröffentlichungen



Innerhalb 12 Monaten

- Meldefristen von IKT-bezogenen Vorfällen und
- weitere Harmonisierung von Instrumenten, Methoden, Prozessen und Strategien für IKT- Risikomanagement (auch Vorgaben für erleichterte Anforderungen)
- Vorgehensweise für die Bewältigung IKT-bezogener Vorfälle (inkl. Schwellenwerten) Allgemeine Grundsätze für die Steuerung des Risikos durch IKT-Drittanbieter



Innerhalb 18 Monaten

- Harmonisierung von Inhalt und Vorlagen von Meldungen
- Erweiterte Prüfungen von IKT-Instrumenten, -Systemen und -Prozessen auf Basis bedrohungsorientierter Penetrationstests
- Wesentliche Vertragsbestimmungen (für Verträge mit IKT-Drittanbietern)
- Harmonisierung der Voraussetzungen für die Durchführung der Aufsicht

Offene Fragen in der Umsetzung

IKT-Drittanbieter



Wie wird die Aufsicht mit Konzentrationsrisiken umgehen?



Wie geht die Aufsicht mit den Hyperscalern um?

Prüfung der digitalen Betriebsstabilität



Wie wird das *Threat Led Penetration Testing* konkret umgesetzt?



Wie wird mit systemischen Erkenntnissen aus den Tests umgegangen?

+

Viele weitere Detailfragen

ISACA Fachgruppe IT-Compliance im Finanz- und Versicherungswesen

Die Fachgruppe vernetzt gezielt ISACA-Mitglieder und Anwender aus dem Finanz- und Versicherungswesen und bietet ihnen ein Forum für den Erfahrungsaustausch im Hinblick auf die Umsetzung dieser Anforderungen.

Hierzu beschäftigt sie sich insbesondere mit

- Bewertung bzw. Kommentierung neuer und überarbeiteter Regularien
- Erarbeitung von Arbeitshilfen zur Umsetzung der Vorgaben
- Diskussion und Erfahrungsaustausch zu Umsetzungen der Vorgaben, Best-Practices und Entwicklung der Regulatorik

Kontakt

E-Mail: fg-it-compliance-fvw@isaca.de

Web: https://www.isaca.de/de/FG_IT_Compliance_FV

Ihre Speaker



Dr. Frank Innerhofer, CISA, CISM, CRISC, CISSP

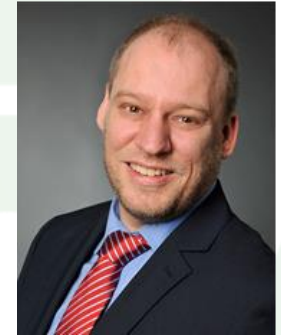
E-Mail: frank.innerhofer@innerhofer.com

LinkedIn: <https://de.linkedin.com/in/frankinnerhofer>

Christian Siepmann, CISM, CDPSE

E-Mail: christian.siepmann@siepmann-infosec.de

LinkedIn: <https://www.linkedin.com/in/christiansiepmann>



Dr. Christian Schwartz, CISM, CRISC, GSTRT

E-Mail: christian.schwartz@usd.de

LinkedIn: <https://www.linkedin.com/in/schwartzc>



ISACA®

Germany Chapter