Digital Operational Resilience Act

Neuerungen und Herausforderungen

24.11.2022

ISACA Germany Chapter

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. Die im November vom Parlament in erster Lesung verabschiedete Fassung baut auf der Kompromissfassung aus dem Juni 2022 auf.

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 im nächsten Jahr relevant werdende Verordnung vorbereiten.

ISACA Germany Chapter

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

\+

Kritische IKT-Drittdienstleister nach einer Definition des Gemeinsamen Ausschusses

ISACA Germany Chapter

Anforderungen an die Governance

Neue Anforderungen

Entscheidende und aktive Rolle des Leitungsorgans bei

- der Steuerung des Rahmens für das IKT-Risikomanagement und
- der Einhaltung einer strikten Cyberhygiene.

Zuweisung angemessener Haushaltsmittel, um den Anforderungen an die digitale Betriebsstabilität gerecht zu werden.

Verpflichtende Fachschulungen für die Mitglieder des Leitungsorgans, um IKT-Risiken und deren Auswirkungen verstehen und bewerten zu können.

Anforderungen sind bisher in Deutschland direkt und indirekt in einschlägiger Gesetzgebung (KonTraG) und den MaRisk enthalten.

ISACA Germany Chapter

Anforderungen an das IKT-Risikomanagement

Systemischer Blick auf das IKT-Risiko

Berücksichtigung von Risiken gegenüber und durch andere Finanzunternehmen.

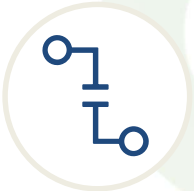
Ermittlung der Vernetzung von IKT-Drittanbietern.

Wiederherstellungszeiten müssen auch potentielle Gesamtauswirkungen auf Markteffizienz berücksichtigen.

Förderung der Resilienz

Neuerungen in Bezug auf Transparenz und Prüfung von BCM auch außerhalb von KRITIS:

- Unabhängige Prüfung von BCM Plänen und
- Übermittlung von Ergebnissen von Notfalltests an Behörden.



Umsetzung automatisierter Mechanismen zur Isolierung von Informationsressourcen und Netzsegmenten.

ISACA Germany Chapter

Mögliche Vereinfachungen und Erleichterungen

Grundsatz der Verhältnismäßigkeit

Art. 4

Anwendung durch die Finanzunternehmen durch Berücksichtigung von deren

- Größe
- Gesamtrisikoprofil
- Art, Umfang, Komplexität ihrer
  - Dienstleistungen,
  - Tätigkeiten,
  - Geschäfte.

Vereinfachter IKT-Risikomanagementrahmen

Art. 16

Ausnahmen von Umsetzung des gesamten IKT-Risikomanagement-rahmens (Art. 5 – Art. 15) für Kleinstunternehmen und weitere bestimmte Unternehmenstypen:

- kleine und nicht-verflochtene Wertpapierfirmen, Zahlungsinstitute, Einrichtungen der betrieblichen Altersversorgung, E-Geld-Institute,
- bzw. weitere festgelegte Institute.

unterliegen **weniger strengen Anforderungen** oder **Ausnahmen**

ISACA Germany Chapter

Meldung IKT-bezogener Vorfälle

Gegenwärtiger Zustand

Nationale Regelungen zur Meldung IKT-bezogener Vorfälle unterscheiden sich teils erheblich, die ENISA Taxonomie ist nicht verbindlich.

Angestrebter Zustand

EU-weite Vereinheitlichung[1] von Meldungen zu IKT-bezogenen Vorfällen und Identifikation und Bemessung des Schweregrads IKT-bezogener Vorfälle.

Zentrale Erfassungs-Plattform soll es ermöglichen schwer-wiegende und weitreichende (evtl. sektorübergreifende) Risiken im EU Finanzwesen zu erkennen.

1. https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

ISACA Germany Chapter

Deep Dive – Meldung IKT-bezogener Vorfälle

Art. 17-21: IKT-bezogene Vorfälle werden nach vorgegebenen Kriterien klassifiziert:

- Zahl der Nutzer / anderen Akteure
- Dauer
- Geografische Ausbreitung
- Mit dem Vorfall verbundene Verluste i.S. von Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit.
- Schwere der Auswirkungen
- Kritikalität betroffener Dienste
- Wirtschaftliche Auswirkungen

ESA entwickeln Schwellenwerte zur Unterscheidung zwischen IKT-bezogenen Vorfällen und schwerwiegenden IKT-bezogenen Vorfällen.

ISACA Germany Chapter

Deep Dive – Meldung IKT-bezogener Vorfälle

Pflicht zur Meldung, ursprünglich direkt vorgeschrieben, nun gemäß RTS

Schwerwiegender IKT-bezogener Vorfälle müssen an die zuständige Behörde gemeldet werden.

Unverzüglich

Initiale Meldung

Spätestens Ende Geschäftstag. Wenn Vorfall 2h vor Ende, 4h nach Beginn des nächsten.

Spätestens nach einer Woche

Zwischenbericht

Gefolgt von Statusaktualisierungen.

Spätestens ein Monat nach erstem Bericht

Abschlussbericht

Nach Ursachenanalyse, unabhängig ob Auswirkungen bislang nur geschätzt oder beziffert wurden. Zuständige Behörde entscheidet dann über Unterrichtung weiterer Behörden.

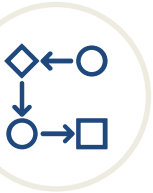
Pflicht zur Unterrichtung von Dienstnutzern und Kunden

Dienstnutzern und Kunden müssen eine Meldung erhalten, falls Auswirkungen auf finanzielle Interessen erfolgt ist oder möglich ist. Eine Folgeunterrichtung über ergriffene Maßnahmen ist notwendig.

ISACA Germany Chapter

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.

ISACA Germany Chapter

Deep Dive – Bedrohungsorientierte Penetrationstests

Im Rahmen von bedrohungsorientierten Penetrationstests wird das Vorgehen von für das Finanzinstitut relevanten Angreifern simuliert.

Unternehmen oder Institute, die nicht den Vereinfachten IKT-Risikomanagementrahmen der DORA anwenden dürfen, müssen bedrohungsorientierte Penetrationstests durchführen, wenn:

- die von dem Institut erbrachten Dienstleistungen einen hohen Einfluss im Finanzsektor haben;
- bedenken bezüglich der Finanzstabilität der Institute bestehen;
- das IKT-Risikoprofil, der IKT-Reifegrad oder technologische Merkmale dies nahelegen.

Die Aufsichtsbehörden erarbeiten in Einvernehmen mit der EZB einen Prozess für die bedrohungsorientierten Penetrationstests auf Basis von TIBER-EU.

ISACA Germany Chapter

Deep Dive – Bedrohungsorientierte Penetrationstests

Der Umfang und das Vorgehen für Bedrohungsorientierte Penetrationstests hängt unter anderem von der Bedeutung der Institute und der beteiligten IKT-Drittdienstleister ab.

- Tests müssen mindestens alle drei Jahre in der Produktivumgebung durchgeführt werden und kritische und wichtige Systeme oder solche, die kritische und wichtige Systeme unterstützen umfassen.
- Alle drei Tests müssen externe Tester eingesetzt werden.

- Die Institute müssen sicherstellen, dass relevante Drittdienstleister in die bedrohungsorientierten Penetrationstests eingebunden sind.
- Für Drittdienstleister besteht die Möglichkeit einen *Pooled-Test* für mehrere betroffene Institute unter der Steuerung eines Instituts durchzuführen.

- Aufsichtsbehörden müssen über das Ergebnis des Tests und die Pläne zur Behebung der Schwächen informiert werden.
- Die Institute erhalten von den Behörden eine Bestätigung des durchgeführten Tests.

ISACA Germany Chapter

IKT-Drittparteienrisiko

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.

Systemischer Blick

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

ISACA Germany Chapter

Deep Dive: Kriterien für kritische IKT-Drittanbieter

Kriterien für kritische IKT-Drittanbieter

- Systemische Auswirkungen auf Stabilität, Kontinuität oder Qualität
- Systemische Bedeutung der Finanz-unternehmen, 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.

Kritischer IKT-Drittanbieter mit Sitz in einem Drittland darf nur dann in Anspruch genommen werden, wenn 12 Monate nach Einstufung seine Eingliederung in die Union mittels Gründung eines Tochterunternehmens vorgenommen wurde.

ISACA Germany Chapter

Informationsaustausch

Betroffene Institute und Unternehmen dürfen Informationen über Cyberbedrohungen austauschen.

Durch den Informationsaustausch muss die Betriebsstabilität erhöht werden.

Der Austausch von Informationen muss in vertrauenswürdigen Gemeinschaften erfolgen.

Der Austausch muss durch ein formelles Abkommen zum Informationsaustausch erfolgen.

Die Finanzinstitute und Unternehmen müssen die Aufsichtsbehörden über den Beitritt oder Austritt aus Informationsaustausch-abkommen informieren.

ISACA Germany Chapter

Zeithorizont

Das EU-Parlament hat im November 2022 in erster Lesung folgende Fassung für DORA verabschiedet. Diese enthält folgende Meilensteine:

Timeline

- **Inkrafttreten DORA**

- Entwürfe für Technische Regulierungsstandards (RTS) und Durchführungs-Standards (ITS)
- Delegierte Verordnungen, unter anderem:
  - Aufsicht über IKT-Drittanbieter
  - Gebühren für freiwillige Prüfungen von IKT-Drittanbieter

- Bericht Machbarkeit zentralisierte Berichterstattung auf EU-Plattform
- Erwartete Anwendung DORA ab Ende 2024

- Entscheidung ob Abschlussprüfer und Prüfungs-gesellschaften ebenfalls Anforderungen DORA an Resilienz unterliegen sollen.

- Zeitraum für Delegierte Rechtsakte Europäische Kommission (Anpassungen)
- Europäische Kommission: Bericht über Kriterien Benennung kritischer IKT-Drittanbieter, ggf. Legislativvorschlag

ISACA Germany Chapter

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

ISACA Germany Chapter

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

ISACA®

Germany Chapter