DORA-Verordnung – VO 2022/2554

Bei diesem Dokument handelt es sich um einen One-Pager, welcher Ihnen darstellt, wie SZR Consulting Ihnen dabei hilft, Ihre Anforderungen zu erfüllen und Ihre Ziele zu erreichen. Weitere Information zu dem Thema können Sie auf unserer Homepage einsehen unter www.SZR-Consulting.com.

Erstellungsdatum: 20.08.2024
Änderungsdatum: 01.05.2025
Version: V1.2

Begriffsbestimmung und rechtliche Grundlage:

Informations- und Kommunikations-Technologie (IKT) stellt eine zentrale Säule in den operationellen Prozessen des Finanzsektors dar. Die DORA-Verordnung und die von der ESMA erstellten L2-Rechtsakte wirken der fehlenden Harmonisierung innerhalb Europas entgegen und stärken die Widerstandsfähigkeit des technischen und operationellen Betriebs im Finanzsektor.

Dabei baut die EU-Kommission mit weiteren Rechtsakten wie NIS2, dem Rechtsakt zur Cybersicherheit, der Cyberresilienz-Verordnung und der Richtlinie zur Resilienz kritischer Einrichtungen ein ausgeweitetes Framework der Cybersicherheit auf, welches auf der Cybersicherheitsstrategie aus dem Jahre 2020 aufbaut.

Die DORA-Verordnung ist dahingehend speziell für den Finanzsektor konzipiert, weshalb sie eine hohe Relevant für Kreditinstitute und Finanzdienstleistungsunternehmen aufweist.

Wir helfen Ihnen dabei, die DORA-Verordnung ordnungsgemäß bei Ihnen zu implementieren**!**

Die Säulen der DORA-Verordnung für den Finanzsektor:

IKT-Risikomanagement

- Gestützt auf Art. 15 und 16 VO 2022/2554 i.V.m. DEL VO 2024/1774 (RTS)
- Finanzunternehmen müssen Standards für Richtlinien, Verfahren, Protokolle und IKT-Sicherheit festlegen, sowie:
  - IKT-Risiken identifizieren und bewerten
  - Implementierung von Sicherheitsmaßnahmen
  - Überwachung von Incidents bzgl. IKT
  - Dokumentation und Berichterstattung

Testing der Resilienz

- Gemäß Art. 24 - 27 VO 2022/2554 haben alle Finanzunternehmen dazu, ihre IKT zu prüfen, indem sie ein risikobasiertes, proportionales Testprogramm etablieren sollen
- Dieses Testing wird auch **Threat-led Penetration Testing (TLPT)** genannt
- Der RTS ist noch nicht im Amtsblatt der EU veröffentlicht

Incident Reporting

- Gestützt auf Art. 18 und Art. 20 VO 2022/2554 müssen Finanzunternehmen Incidents klassifizieren und als "relevant" identifizieren
- Finanzunternehmen müssen relevante Incidents reporten gemäß DEL VO 2024/2956 und DEL VO 2024/1773
  - Initial Report nicht länger als 24 Stunden
  - Intermediate Report nach 72 Stunden
  - Final Report bis zu 1 Monat nach dem letzten Intermediate Report

Managerment der IKT-Dienstleiter

- Finanzunternehmen haben ein Inventar ihrer IKT-Dienstleister zu führen und an die BaFin zu reporten (gestützt auf DEL VO 2024/2956 (RTS))
- Die Verträge mit IKT-Dienstlesiter haben hohe Anforderungen zu erfüllen und Unternehmen haben eine Strategie für das Management der IKT-Dienstleister festzuhalten; inklusive einer Exit Strategie (DEL VO 2024/1773 (RTS))

Informationsteilung

- Gemäß Art. 45 VO 2022/2554 können Finanzunternehmen Erkennisse über Cyberbedrohungen untereinander austauschen
- Dazu sind Vereinbarungen über den Austausch zu Cybebedrohungen augzusetzen

Aktuelles: Kritische und ausstehende Fragen zur DORA-Verordnung:

Die meisten L2-Rechtsakte sind bereits im Amtsblatt der Europäischen Union veröffentlicht. Die Veröffentlichung zu weiteren Informationen zum **Threat-led Penetration Testing** sind noch nicht offen.

Des Weiteren sind aktuell noch der L2-Rechtsakt gemäß Art. 30.5 VO 2022/2554 offen, wonach die Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen zu bestimmen sind.

Als nächster wichtiger Schritt (nachdem Finanzunternehmen ihr Informationsregister gemäß Art. 28 VO 2022/2554 an die BaFin übermittelt haben), werden gemäß DEL VO 2024/1173 die ESA´s entscheiden, welche IKT-Dienstleister als „kritisch“ zu bewerten sind; CTPP (critical ICT third-party service provider). IKT-Diensterleister erhalten daraufhin die Information der ESA´s und können zu diesem Schreiben Stellung beziehen.

Entsprechend gibt es noch offene Fragen zur DORA-Verordnung, weshalb es wichtig ist, dass Finanzunternehmen stetig über die neueste Änderung informiert werden.

So unterstützen wir Sie:

Methodisch:

- Projekt-Management und Projekt-Leitung
- Business-Analyse
- PMO
- Change-Management
- Requirements-Engineering

Fachlich:

- Implementierung von DORA-Anforderungen
- Überprüfung von IKT-Dienstleister-Verträgen
- Implementierung des IKT-Dienstleiter-Inventars
- Implementierung des Incident-Reporting
- Aufbau von Informationsaustausch zu Cyberbedrohungen

Operativ:

- Unterstützung bei der Klassifizierung und Meldung von Incidents
- Unterstützung bei der Aufrechterhaltung des Inventars von IKT-Dienstleister
- Unterstützung bei der Überprüfung von Verträgen mit IKT-Dienstleistern

Kontaktieren Sie uns gerne!

Thomas-Marc.Szroeter@SZR-Consulting.com
+49 176 207 44 990
www.SZR-Consulting.com

Mit freundlichen Grüßen
Thomas-Marc Szroeter