DORA – die vier Handlungsfelder für Banken

Ihr Monitoring: **IKT-Risikomanagement**

1

- Technische und organisatorische Fähigkeiten eines Finanzunternehmens, die auf die Sicherheit der IKT-Systeme abzielen (personelle Ausstattung, Fachwissen, Verhaltensregeln für Mitarbeitende und organisatorische Regelungen)
- Gesamtüberblick über alle Risiken im Zusammenhang mit Informations- und Kommunikationstechnik (IKT)
- Einrichtung einer IKT-Risikokontrollfunktion (die auch auslagerbar ist)
- Transparenz im Informationsverbund: Welche IKT-Systeme werden genutzt und wofür? Risiken der IKT-Drittdienstleister müssen transparent sein und in das eigene Risikomanagement mit eingebracht werden.

Und wenn der Fall eintritt: **Management IKT-bezogener Vorfälle**

2

- Erkennung, Meldung und Behandlung von IKT-Vorfällen
- Kontinuierliche Verbesserung interner Prozesse im IKT-Risikomanagement und gegenseitiges Lernen durch Informationsaustausch zwischen den Finanzunternehmen für bessere Sicherheits- und Abwehrmaßnahmen

DORA
(Digital Operational Resilience Act)

Einheitlicher Rahmen für ein effektives und umfassendes Management von Cybersicherheits- und IKT-Risiken auf den Finanzmärkten

Auf Herz und Nieren: **Testen der digitalen, operationalen Resilienz**

3

- Systeme werden hinsichtlich ihrer Anfälligkeiten und ihrer Resilienz im Falle eines Angriffs überprüft. Dabei wird die Ausfallsicherheit unter Realbedingungen getestet.
- Auch Lösungen Dritter werden in die Tests einbezogen.

Alles im Blick haben: **IKT-Drittparteien-Risikomanagement**

4

- Transparenz der Anhängigkeit von IKT-Drittdienstleistern: Banken müssen alle IKT-Dienstleister im Informationsregister führen. Auf europäischer Ebene erfolgt eine zentrale Überwachung von IKT-Drittdienstleistern, die für viele Finanzunternehmen kritische und wichtige Funktionen erbringen.
- Die IKT-Risiken der Dienstleister müssen den Banken gegenüber transparent sein und mitbewertet werden.
- Vertragliche Vereinbarungen mit IKT-Drittdienstleistern müssen detailliert beschrieben werden.
- Kritisch für Finanzunternehmen sind IKT-Drittdienstleister, die in Finanzunternehmen kritische und wichtige Funktionen erbringen.

Inkrafttreten der DORA-Verordnung und der Änderungsrichtlinie am 17. Januar 2023