DORA – Digitale Resilienz in der Finanzwelt

WORUM GEHT ES?

- ➔ Die EU hat den Digital Operational Resilience Act (DORA) zur Verbesserung der Widerstandsfähigkeit des Finanzsektors gegenüber digitalen Risiken veröffentlicht.
- ➔ DORA ist am 16.01.2023 in Kraft getreten und ab dem 17. 01.2025 anzuwenden.
- ➔ Die Verordnung ist ein detailliertes und umfassendes Rahmenwerk für die digitale Betriebsstabilität von EU-Finanzunternehmen mit 3 Kernzielen:
  - Vereinheitlichung und Erweiterung bestehender europäischer und nationaler Standards an die Sicherheit der Informations- und Kommunikationstechnik (IKT)
  - Sicherstellung einer ausreichenden Absicherung gegen digitale Risiken
  - Etablierung eines Rechtsrahmens für die Überwachung von IKT-Drittanbietern

WAS IST NEU?

- Umfassende Strategien und Richtlinien zum Management von IKT-Risiken und Übertragung der Gesamtverantwortung an den Vorstand bzw. die Geschäftsführung
- Etablierung von Prozessen zur Erkennung, Evaluierung und Meldung von IKT-Vorfällen
- Erhöhte Anforderungen an Teststrategien und Testverfahren, insbesondere an bedrohungsorientierte Penetrationstests
- Integration des IKT-Drittparteienrisikos in die Unternehmensstrategie und -prozesse, wodurch neue Anforderungen u.a. an das Auslagerungsmanagement entstehen
- Kritische IKT-Dienstleister können direkt von den Aufsichtsbehörden reguliert werden
- (Opt.) Direkter Informationsaustausch der Finanzunternehmen zu Cyberbedrohungen

WAS SOLLTEN SIE TUN?

- IKT-Risikomanagement: Etablierung eines geeigneten Governance- und Kontrollrahmens für das Management von IKT-Risiken und der digitalen Resilienz
- Reaktion auf IKT-Vorfälle: Etablierung von Prozessen und Standards zur Erkennung, Evaluierung und Meldung an die zuständige Aufsichtsbehörde (BaFin)
- Testverfahren: Einführung von geeigneten, unabhängigen Tests gemäß den regulatorischen Vorgaben zur Verbesserung der digitalen Resilienz
- Management des IKT-Drittparteienrisikos: risikoorientierte Überwachung und Management der IKT-Drittparteien vor, während und nach Vertragsschluss

WAS KÖNNEN WIR FÜR SIE TUN?

- Scope-Analyse der DORA-Betroffenheit und (IST-)Analyse zur Identifizierung vorhandener Gaps sowie die Ableitung und Darstellung von Handlungsempfehlungen
- Konzepterstellung zur fachlichen und technischen Umsetzung
- Administrative, fachliche und technische Unterstützung der Umsetzung
- Operative Durchführung unabhängiger Penetrationstests gemäß aktuellen Standards
- Operative Unterstützung bei der Analyse, Auswertung und Berichterstattung von IKT-Vorfällen

Für Fragen oder Anmerkungen melden Sie sich gerne per E-Mail: armin.binsteiner@concedro.com.