DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

Der Digital Operational Resilience Act (DORA), eine Verordnung der EU, ist am 16.01.2023 in Kraft getreten. Die Umsetzungsfrist endet am 17.01.2025. Bis dahin haben Unternehmen im Finanzsektor die in der DORA-Verordnung einheitlich formulierten Anforderungen zur Stärkung der digitalen operationalen Resilienz zu erfüllen.

Grundsätzlich gilt DORA – bis auf wenige Ausnahmen - für alle Finanzunternehmen und formuliert sektorübergreifend einheitliche Anforderungen an die Cyber-Sicherheit. Die bestehenden regulatorischen Anforderungen der BaFin im Bereich Informationssicherheit wie BAIT, VAIT, KAIT oder ZAIT sollen, um Dopplungen zu vermeiden, entsprechend angepasst werden.

Die DORA-Verordnung unterstreicht die Notwendigkeit für Finanzunternehmen, den Risiken durch Digitalisierung und der damit einhergehenden, starken Abhängigkeit von der Informations- und Kommunikationstechnologie (IKT) mit einer angemessenen Organisation und dem erforderlichen internen Kontrollsystem (IKS) zu begegnen.

Die in DORA formulierten, regulatorischen Anforderungen lassen sich fünf Themengebieten zuordnen:

- IKT-Risikomanagement inkl. IKT-Governance
- Behandlung, Klassifizierung und Berichterstattung von IKT-Vorfällen
- Testen der digitalen operationalen Resilienz
- Management des IKT-Drittparteirisikos
- Überwachungsrahmen für kritische IKT Drittdienstleister

Die DORA-Verordnung fasst Anforderungen aus bestehenden Verordnungen der BaFin – Stichwort VAIT, BAIT, KAIT und ZAIT - sowie des BSI – Stichwort KRITIS - auf und ergänzt diese um neue Elemente wie das Überwachungsrahmenwerk für kritische IKT Drittdienstleister.

KONKRETISIERUNG ERFOLGT IN RTS UND ITS

Bis zum Ablauf der Umsetzungsfrist werden die in DORA formulierten, regulatorischen Anforderungen in 13 weiteren EU-Rechtsakten entweder als technischer Regulierungsstandard (Regulatory Technical Standard (RTS)) oder als technischer Durchführungsstandard (Implementing Technical Standard (ITST)) konkretisiert. Die European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) haben kürzlich die ersten 4 RTS sowie den ersten ITS im Entwurf zur Konsultation veröffentlicht.

REGULATORY ASSURANCE: DER BDO UNTERSCHIED

Unser IT & Controls Assurance-Team hilft Ihnen mit interdisziplinärer Expertise aus Prüfungs- und Beratungsprojekten, den Stand der Umsetzung im Unternehmen zu erarbeiten sowie Optimierungspotential zu erkennen und zu verstehen. Gemeinsam mit Ihnen diskutieren wir geeignete Maßnahmen, um Ihnen eine schnelle und effiziente Umsetzung zu ermöglichen. Angefangen auf strategischer Ebene, über taktische Maßnahmen bis hin zu operativen Prozessen.

ÜBER BDO

BDO zählt mit über 2.500 Mitarbeitern an 27 Offices zu den führenden Gesellschaften für Wirtschaftsprüfung und prüfungsnahe Dienstleistungen, Steuerberatung und wirtschaftsrechtliche Beratung sowie Advisory in Deutschland.

Die BDO AG Wirtschaftsprüfungsgesellschaft ist Gründungsmitglied von BDO International (1963), der mit heute über 111.000 Mitarbeitern in 164 Ländern einzigen weltweit tätigen Prüfungs- und Beratungsorganisation mit europäischen Wurzeln.

www.bdo.de

KONTAKT

BDO AG
Wirtschaftsprüfungsgesellschaft

KARSTEN THOMAS
Partner, IT & Controls Assurance
Telefon: +49 2111371277
karsten.thomas@bdo.de

FELIX KRAMER
Senior Manager, IT & Controls Assurance
Telefon: +49 8976906232
felix.kramer@bdo.de

07/2023